PRIMEQUEST 500A/500/400-Modellreihe

Installationshandbuch

Bitte beachten Sie die Table of corrections (errata) 2009/6/18 am Handbuchende.

Ausgabe April 2008 *(Errata 2006/10/10, 2008/09/19, 2008/12/18 und 2009/02/24 eingearbeitet)* Bitte

Kritik… Anregungen… Korrekturen…

Die Redaktion ist interessiert an Ihren Kommentaren zu diesem Handbuch. Ihre Rückmeldungen helfen uns, die Dokumentation zu optimieren und auf Ihre Wünsche und Bedürfnisse abzustimmen.

Für Ihre Kommentare stehen Ihnen Fax-Formulare auf den letzten Seiten dieses Handbuchs zur Verfügung.

Dort finden Sie auch die Adressen der zuständigen Redaktion.

Copyright und Handelsmarken

Copyright © FUJITSU LIMITED and FujitsuTechnology Solutions GmbH 2005 - 2009.

Alle Rechte vorbehalten.
Liefermöglichkeiten und technische Änderungen vorbehalten.

Alle verwendeten Hard- und Softwarenamen sind Handelsnamen und/oder Warenzeichen der jeweiligen Hersteller.

Umweltschutz und Service

Die PRIMEQUEST-Systeme besitzen eine lange Lebensdauer. Nicht nur die Erweiterungsmöglichkeiten, sondern auch die Qualität geben dafür den Ausschlag.

Die Entwicklung geht jedoch weiter. Heute kaum abzusehende Datenmengen müssen in Zukunft verarbeitet werden. Die Ansprüche an Speicherplatz, Geschwindigkeit und Design der Computer steigen. Es kommt der Zeitpunkt, an dem Ihr PRIMEQUEST-System durch ein Nachfolgemodell ersetzt und das alte Gerät entsorgt werden muss. Auch hier bietet unser Unternehmen Unterstützung an.

Bei Fujitsu Technology Solutions hat Recycling von Computer-Altgeräten bereits Tradition: Seit vielen Jahren werden ausgediente Computer zurückgenommen und verwertet. Bereits bei der Konstruktion wird auf die Wiederverwendbarkeit von Einbauteilen und auf die Wiederverwertbarkeit von Materialien besonderer Wert gelegt.

Auch Ihr PRIMEQUEST-System ist weitestgehend aus Materialien hergestellt, die einem fachgerechten Recycling zugeführt bzw. umweltschonend entsorgt werden können.

Lesen Sie hierzu auch die folgenden Abschnitte, in denen unsere Maßnahmen zum Schutz der Umwelt kurz erläutert sind, die darüber hinaus aber auch Anregungen und Tipps enthalten, die den umweltgerechten Einsatz des Systems bei Ihnen ermöglichen.

Umweltgerechte Produktgestaltung und -entwicklung

Dieses Produkt wurde nach Fujitsu Technology Solutions Richtlinie FSC 03230 „Umweltgerechte Produktgestaltung und -entwicklung“ konzipiert.

Das bedeutet, dass entscheidende Kriterien wie Langlebigkeit, Materialauswahl und -kennzeichnung, Emissionen, Verpackung, Demontagefreundlichkeit und Recyclingfähigkeit berücksichtigt wurden.

Dies schont Ressourcen und entlastet somit die Umwelt.

Die Entwicklungs- und Produktionsbereiche der PRIMEQUEST-Systeme wurden nach dem Umweltmanagementsystem DIN ISO 14001 zertifiziert.

Hinweis zum sparsamen Energieverbrauch

Bitte schalten Sie Geräte, die nicht ständig eingeschaltet sein müssen, erst bei Gebrauch ein, sowie bei längeren Pausen und bei Arbeitsende wieder aus.

Hinweis zum Umgang mit Verbrauchsmaterialien

Bitte entsorgen Sie Drucker-Verbrauchsmaterialien und Batterien gemäß den landesrechtlichen Bestimmungen.

Hinweis zu Aufklebern auf Kunststoff-Gehäuseteilen

Bitte kleben Sie möglichst keine eigenen Aufkleber auf Kunststoff-Gehäuseteile, da diese das Recycling erschweren.

Rücknahme, Recycling und Entsorgung

Unser Wiedervermarktungs und Recyclingzentrum ist nach der Öko-Audit-Verordnung der Europäischen Gemeinschaft zertifiziert. Hier erfahren Sie Einzelheiten zur Rücknahme und Verwertung der Geräte und Verbrauchsmaterialien im europäischen Raum:

Tel. +49 (0) 5251 8 18010
Fax +49 (0) 5251 8 18015
URL http://www.ts.fujitsu.com/recycling

Ihre Fujitsu Technology Solutions Geschäftsstelle berät Sie ebenfalls.

Service

Bei Reklamationen wegen fehlender/nicht funktionierender Teile wenden Sie sich bitte an die Reklamationsabteilung von Fujitsu Technology Solutions:

Tel. +49 (0) 5251 8 22222
Fax +49 (0) 5251 8 22029

Außerdem können auch über das Internet Reklamationen gemeldet werden:

http://abgadwda.abg.fsc.net/RLC/
Email: RLC@ts.fujitsu.com

Wenn Sie einmal ein Problem mit Produkten von Fujitsu Technology Solutions haben, oder wenn sich Fragen zum Aufstellen oder zum Betrieb ergeben: unsere Support-Spezialisten können schnelle und kompetente Unterstützung anbieten:
http://www.ts.fujitsu.com/support/helpdesk.html

Unter dieser Adresse finden Sie auch Rubriken zu Produkten, Telefon-Nummern, etc.

In Deutschland ist das Call Management Center (CMC) unter folgenden Nummern zu erreichen:

Tel. +49 01805 4040
Fax +49 01805 336779

DE	Dieses Gerät ist entsprechend der europäischen Richtlinie 2002/96/EG über Elektro- und Elektronikaltgeräte (waste electrical and electronic equipment - WEEE) gekennzeichnet. Die Richtlinie gibt den Rahmen für eine EU-weit gültige Rücknahme und Verwertung der Altgeräte vor.
EN	This appliance is labelled in accordance with European Directive 2002/96/EG concerning used electrical and electronic appliances (waste electrical and electronic equipment - WEEE). The guideline determines the framework for the return and recycling of used appliances as applicable throughout the EU.
AR	ةمءيدقلا ةيئابرهكلاو ةينورتكلإلا ةياقبلا ةيبرولأا ةيداصتقالا ةعومجملا/2002/96 ةيبرولأا ةفصاوملل قباطم زاهجلا اذه (waste electrical and electronic equipment - WEEE). .امل‌الغتسا ةداعإو ةمءيدقلا ةزهجألا ةداعتسا صوصخب يبرولأا داحتالا لود ليمعي يف ةريسي دعاوقل لماعلا راطلا ددحت ةفصاوملا هذهو
BG	Този уред е обозначен в съответствие с европейската директива 2002/96/EG за стари електрически и електронни уреди (waste electrical and electronic equipment - WEEE). Тази директива регламентира валидните в рамките на ЕС правила за приемане и използване на стари уреди
CS	Tento spotřebič je označen v souladu s evropskou směrnicí 2002/96/EG o nakládání s použitými elektrickými a elektronickými zařízeními (waste electrical and electronic equipment - WEEE). Tato směrnice stanoví jednotný evropský (EU) rámec pro zpětný odběr a recyklování použitých zařízení.
DA	Dette apparat er klassificeret iht. det europæiske direktiv 2002/96/EF om affald af elektrisk- og elektronisk udstyr (waste electrical and electronic equipment - WEEE). Dette direktiv angiver rammerne for indlevering og recycling af kasserede apparater gældende for hele EU.
EL	Αυτή η συσκευή χαρακηρίζεται σύμφωνα με την ευρωπαϊκή οδηγία 2002/96/ΕΚ περί ηλεκτρικών και ηλεκτρονικών συσκευών (waste electrical and electronic equipment - WEEE). Η οδηγία προκαθορίζει τα πλαίσια για μια απόσυρση και αξιοποίηση των παλιών συσκευών με ισχύ σ' όλη την ΕΕ.
ES	Este aparato está marcado con la Directiva europea 2002/96/CE relativa al uso de aparatos eléctricos y electrónicos (Residuos de aparatos eléctricos y electrónicos). La directiva proporciona el marco general válido en todo el ámbito de la Unión Europea para la retirada y la reutilización de los residuos de los aparatos eléctricos y electrónicos.
ET	Käesolev seade on märgistatud vastavalt direktiivile 2002/96/EÜ elektri-ja elektroonikaseadmete jäätmete kohta. Direktiiv sätestab elektri- ja elektroonikaseadmete jäätmete tagastamise ja ringlussevõtu raamtingimused Euroopa Liidus.
FA	یکیترونکلا و یقرب نمک یاه هاگتسد مراب رد 2002/96/EG یئاپورا طباوض قباطم هاگتسد نیا ((waste electrical and electronic equipment - WEEE .تسا هدش صخشم .دنک یم نییعت ار نمک یاه هاگتسد تفایزاب و نتفرگ سپزاب هویش یلک بوچ راچ، تسا ربتعم اپوا رسارس رد هک طباوض نیا
FI	Tämän laitteen merkintä perustuu käytettyjä sähkö- ja elektroniikkalaitteita (waste electrical and electronic equipment - WEEE) koskevaan direktiiviin 2002/96/EG. Tämä direktiivi määrittää käytettyjen laitteiden palautus- ja kierrätys-säännökset koko EU:n alueella.
FR	Cet appareil est marqué selon la directive européenne 2002/96/CE relative aux appareils électriques et électroniques usagés (waste electrical and electronic equipment - WEEE). La directive définit le cadre pour une reprise et une récupération des appareils usagés applicables dans les pays de la CE.
HE	שומישמ ואציש מיירושכמ רובע 2002/96/EG תיפוריאה הייחנהל מאתהב רדגומ הז רישכמ (waste electrical and electronic equipment - WEEE). .שומישמ ואציש מירישכמ לש הכרעהו הרזח הלבקל ,יפוריאה דוחיאה ללכ רובע הפקת ,תרגסמ הרידגמ הייחנהה
HR	Ovaj je uređaj označen u skladu s europskom smjernicom 2002/96/EG o otpadnim električnim i elektronskim uređajima (waste electrical and electronic equipment - WEEE). Smjernica određuje okvir za povratak i zbrinjavanje otpadnih uređaja valjan u cijeloj Europskoj Uniji.
HU	Ez a készülék az elhasznált villamossági és elektronikai készülékekről szóló 2002/96/EK irányelvnek megfelelő jelölést kapott. Ez az irányelv a már nem használt készülékek visszavételének és hasznosításának EU-szerte érvényes kereteit határozza meg.
IT	Questo apparecchio dispone di contrassegno ai sensi della direttiva europea 2002/96/CE in materia di apparecchi elettrici ed elettronici (waste electrical and electronic equipment - WEEE). Questa direttiva definisce le norme per la raccolta e il riciclaggio degli apparecchi dismessi valide su tutto il territorio dell'Unione Europea.
KO	이 기기는 폐기처리하게되는 전기/전자장치 (waste electrical and electronic equipment - WEEE)에 대한 유럽 기준 2002/96/EG 에 상응하게 표시되어 있습니다. 이 기준은 EU 국가에서의 폐기처리하게되는 기기의 회수와 재활용에 대한 범위를 정의합니다.
LT	Šis prietaisas yra pažymėtas pagal Europos bendrijos direktyvą 2002/96/EG dėl naudotų elektrinių ir elektroninių prietaisų (waste electrical and electronic equipment - WEEE). Ši direktyva apibrėžia visoje ES galiojančią naudotų prietaisų grąžinimo ir perdirbimo tvarką.
LV	Šī ierīce ir marķēta atbilstoši Eiropas direktīvai 2002/96/EG par elektriskajām un elektroniskajām ierīcēm (waste electrical and electronic equipment – WEEE). Direktīva nosaka veidu, kā ES teritorijā jārealizē nolietoto ierīču nodošana un pārstrāde.

MK	Овој апарат е означен според европскиот пропис 2002/96/E3 за електро и електронски апарати (waste electrical and electronic equipment – WEEE). Прописот ја дава рамката за враќање и искористување на старите апарати, важечко ширум Европа.
MS	Alat ini bersesuaian dengan garis panduan Eropa 2002/96/EG tentang alat-alat tua elektrik dan elektronik (waste electrical and electronic equipment - WEEE) . Garis panduan tersebut memberi rangka rujukan yang berlaku di seluruh Eropa untuk penerimaan balik dan penggunaan alat-alat tua.
NL	Dit apparaat is gekenmerkt in overeenstemming met de Europese richtlijn 2002/96/EG betreffende afgedankte elektrische en elektronische apparatuur (waste electrical and electronic equipment - WEEE). De richtlijn geeft het kader aan voor de in de EU geldige terugneming en verwerking van oude apparaten.
NO	Dette apparatet er klassifisert i henhold til det europeiske direktivet 2002/96/EF om avhending av elektrisk- og elektronisk utstyr (waste electrical and electronic equipment – WEEE). Direktivet angir rammene for innlevering og gjenvinning av innbytteprodukter.
PL	Urządzenie to oznaczono zgodnie z europejską wytyczną 2002/96/EG o zużytych urządzeniach elektrycznych i elektronicznych (waste electrical and electronic equipment - WEEE). Wytyczna ta określa ramy obowiązującego w całej Unii Europejskiej odbioru i wtórnego wykorzystania starych urządzeń.
PT	Este aparelho está marcado em conformidade com a Directiva 2002/96/CE relativa aos resíduos de equipamentos eléctricos e electrónicos (waste electrical and electronic equipment - WEEE). A directiva estabelece o quadro para a criação de um sistema de recolha e valorização dos equipamentos usados válido em todos os Estados Membros da União Europeia.
RO	Acest aparat este marcat corespunzător directivei europene 2002/9/CE în privinţa aparatelor electrice şi electronice vechi (waste electrical and electronic equipment – WEEE). Directiva prescrie cadrul pentru o preluare înapoi, valabilă în întreaga UE, şi valorificarea aparatelor vechi.
RU	Данный прибор имеет отметку о соответствии европейским нормам 2002/96/EG утилизации электрических и электронных приборов (waste electrical and electronic equipment - WEEE). Данные нормы определяют действующие на территории Евросоюза правила возврата и утилизации старых приборов.
SK	Tento spotrebič je označený v súlade s európskou smernicou 2002/96/EG o nakladaní s použitými elektrickými a elektronickými zariadeniami (waste electrical and electronic equipment - WEEE). Táto smernica stanoví jednotný európsky (EU) rámec pre spätný odber a recyklovanie použitých zariadení.
SL	Ta naprava je označena v skladu z evropsko smernico o odpadni električni in elektronski opremi (waste electrical and electronic equipment - WEEE). V okviru smernice sta določena prevzem in recikliranje starih naprav, ki veljata v celotni Evropski uniji.
SQ	Ky aparat përmban shënjën e aparaturave elektrike dhe elektroteknike sipas Udhëzimit 2002/96/EG (waste electrical and electronic equipment - WEEE). Udhëzimi jep kuadrin ligjor për te drejtën e kthimit mbrapsht të aparaturave të përdorura në të gjithë BE.
SR	Ovaj je aparat označen u skladu sa evropskom smernicom 2002/96/EG o otpadnim električnim i elektronskim aparatima (waste electrical and electronic equipment - WEEE). Smernica određuje okvir za povratak i reciklažu otpadnih aparata koji važi u celoj Evropskoj Uniji.
SV	Denna enhet är märkt i enlighet med der europeiska direktivet 2002/96/EG om avfall som utgörs av eller innehåller elektroniska produkter (waste electrical and electronic equipment - WEEE). Direktivet anger ramarna för inom EU giltigt återtagande och korrekt återvinning av uttjänta enheter.
TH	อุปกรณ์นี้ได้มาตรฐานตาม European Guideline 2002/96/EG ว่าด้วยการทำเครื่องหมายอุปกรณ์ไฟฟ้า-อิเล็กทรอนิกส์เก่า (การกำจัดทิ้งอุปกรณ์ไฟฟ้า-อิเล็กทรอนิกส์ – WEEE) ซึ่งใช้เป็นแนวทางสำหรับสหภาพยุโรปในการยกเลิกการใช้งานและการใช้งานอุปกรณ์ไฟฟ้า-อิเล็กทรอนิกส์เก่าอย่างถูกต้อง
TR	Bu cihaz, ömrünü doldurmuş elektrikli ve elektronik cihazlar ile ilgili Avrupa yönetmeliği 2002/96/EG'ye (waste electrical and electronic equipment – WEEE) uygun şekilde işaretlenmiştir. Bu yönetmelik, eski cihazların geri alımı ve değerlendirilmesi ile ilgili AB-çapındaki uygulamaların çerçevesini belirtmektedir.
UK	Цей прилад маркіровано згідно положень європейської Директиви 2002/96/EG стосовно електронних та електроприладів, що були у використанні (waste electrical and electronic equipment - WEEE). Директивою визначаються можливості, які є дійсними у межах Європейського союзу, щодо прийняття назад та утилізації бувших у використанні приладів.
ZF	本設備說明是根據歐洲電子及電氣舊設備準則 2002/96/EG（廢棄電子及電氣設備 WEEE）。 此準則提供於歐盟成員對舊設備之報廢或使用標準。
ZH	对本设备根据有关电气和电子设备报废的欧洲规定 2002/96/EG（waste electrical and electronic equipment – WEEE）进行标记。 该规定管理在欧洲范围内对报废设备的回收和再生。

SICHERER BETRIEB DES SYSTEMS

Das vorliegende Handbuch enthält wichtige Informationen zum Einsatz und zur Handhabung dieses Produkts. Lesen Sie das Handbuch sorgfältig durch. Beachten Sie insbesondere das Kapitel „SICHERHEITSHINWEISE“. Benutzen Sie das Produkt nur entsprechend den Anweisungen und Informationen in diesem Handbuch. Halten Sie das Handbuch bereit, um es weiterhin heranzuziehen.
Fujitsu und Fujitsu Technology Solutions treffen erforderliche Vorkehrungen, um zu vermeiden, dass Benutzer und andere Personen verletzt werden oder deren Eigentum beschädigt wird. Verwenden Sie dieses Produkt dem vorliegenden Handbuch gemäß.

WICHTIGER HINWEIS ZU DIESEM PRODUKT

Dieses Produkt wurde für allgemeine Anwendungsgebiete entworfen und hergestellt, wie z. B. für den Einsatz im Büro, in Verwaltungen und für allgemeine industrielle Anwendungen. Das Produkt ist nicht vorgesehen für den Einsatz in Steuerungssystemen für Kernreaktoren, in Luftnavigations- und Weltraumsystemen, in Systemen zur Steuerung und Überwachung des Luftverkehrs und von Massentransportmitteln, an lebensunterstützenden Geräten der Medizin, zur Steuerung der Abschussvorrichtungen von Flugkörpern oder für andere besondere Anwendungsbereiche, in denen außerordentlich hohe Zuverlässigkeitsanforderungen gestellt werden. In diesen Einsatzbereichen kann das erforderliche Sicherheitsniveau entweder nicht garantiert werden, oder eine Fehlfunktion oder Betriebsstörung könnte sich lebensbedrohend auswirken oder zur Verletzung von Personen führen. (Diese sicherheitskritischen Einsatzbereiche werden nachstehend als „Einsatzbereiche mit hohem Risiko“ bezeichnet.) Sie dürfen das Produkt nicht in einem Einsatzbereiche mit hohem Risiko verwenden, ohne die erforderliche Sicherheit zu gewährleisten. Falls Sie dieses Produkt in einem Einsatzbereiche mit hohem Risiko verwenden wollen, wenden Sie sich vor dem Einsatz an zuständige Vertriebsrepräsentanten.

FCC-HINWEIS

Der folgende Hinweis gilt nur für Benutzer in der EU.

WARNUNG: Dieses Produkt entspricht der Geräteklasse A der Europanorm EN55022. Bei Installation in Innenräumen verursacht dieses Gerät möglicherweise Funkstörungen, zu deren Behebung der Benutzer gegebenenfalls geeignete Maßnahmen ergreifen muss.

Der folgende Hinweis gilt nur für Benutzer in den USA.

Dieses Gerät wurde getestet und befindet sich gemäß Teil 15 der FCC-Regeln innerhalb der Grenzen der Geräteklasse A gemäß Teil 15 der FCC-Richtlinien. Diese Grenzen sind zur Herstellung eines angemessenen Schutzes gegen schädliche Störstrahlung bei Installation in Geschäftsäumen konzipiert. Von diesem Gerät wird Energie im Radiofrequenzbereich erzeugt, verwendet, und möglicherweise abgestrahlt.
Bei nicht anweisungsgemäßer Installation und Benutzung kann es zu Beeinträchtigungen des Funkverkehrs kommen. Bei Betrieb dieses Gerätes in einem Wohngebiet kommt es wahrscheinlich zu Störungen. Die Maßnahmen zu deren Beseitigung muss der Anwender auf eigene Kosten ergreifen.

Laser-Standards

In diesem Gerät befinden sich Laser-Produkte der Klasse 1. Es erfüllt die Anforderungen der FDA Radiation Performance Standards 21 CFR 1040.10 und 1040.11 sowie der International Laser Safety Standards IEC60825-1: 2001.

WARENZEICHEN

- Microsoft, Windows, MS, Windows NT und Windows Server sind Warenzeichen oder eingetragene Warenzeichen der Microsoft Corporation in den Vereinigten Staaten und/oder in anderen Ländern.
- Linux ist ein Warenzeichen oder eingetragenes Warenzeichen von Linus Torvalds in den Vereinigten Staaten sowie in anderen Ländern.
- Red Hat, RPM und alle auf Red Hat basierenden Warenzeichen und Logos sind in den Vereinigten Staaten sowie in anderen Ländern Warenzeichen oder eingetragene Warenzeichen Red Hat, Inc.
- SUSE ist ein Warenzeichen der Novell, Inc. in den Vereinigten Staaten und anderen Ländern.
- Intel, Xeon und Itanium sind Warenzeichen oder eingetragene Warenzeichen der Intel Corporation.
- Ethernet ist ein eingetragenes Warenzeichen der Fuji Xerox Co., Ltd. und der Xerox Corporation in den Vereinigten Staaten sowie in anderen Ländern.
- Alle anderen in diesem Handbuch genannten Produktnamen sind Warenzeichen bzw. eingetragene Warenzeichen der jeweiligen Inhaber.
- Die System- und Produktnamen in diesem Handbuch sind nicht in jedem Fall mit den Symbolen für Warenzeichen (™) bzw. eingetragene Warenzeichen (®) gekennzeichnet.

NUTZUNGSBEDUINGUNGEN FÜR SOFTWARE VON DRITTANBIETERN

Das Produkt enthält neben der von Fujitsu Ltd. oder von Fujitsu Technology Solutions GmbH bereitgestellten Software auch Software von Drittanbietern. Es ist Ihnen erlaubt, die Software der Drittanbieter gemäß den nachfolgenden Geschäftsbedingungen zu nutzen. Falls Sie sich den Quellcode für die Software beschaffen, auf die die nachfolgenden Geschäftsbedingungen angewendet werden, wird hiermit auf „LICENSE1_EN.pdf“ und „LICENSE2_EN.pdf“ verwiesen, die Sie auf http://manuals.ts.fujitsu.com/ finden.

DIESE SOFTWARE WIRD IM VORLIEGENDEN ZUSTAND BEREITGESTELLT UND FUJITSU LIMITED UND FUJITSU TECHNOLOGY SOLUTIONS GMBH ÜBERNEHMEN WEDER AUSDRÜCKLICH NOCH STILLSCHWEIGEND IRGENDEINE GEWÄHRLEISTUNG FÜR DIESE SOFTWARE; DIES SCHLIEßT ALLE GEWÄHRLEISTUNGEN FÜR DIE MARKTGÄNGIGKEIT ODER DIE EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UNEINGESCHRÄNKT EIN.

FUJITSU LIMITED UND FUJITSU TECHNOLOGY SOLUTIONS HAFTEN IN KEINEM FALL FÜR ANSPRÜCHE DURCH DRITTE ODER FÜR BESONDERE ODER INDIREKTE SCHÄDEN, FOLGESCHÄDEN ODER SONSTIGE SCHÄDEN, DIE AUS NUTZUNGSAUSFALL, DATENVERLUST ODER ENTGANGENEM GEWINN RESULTIEREN - SEI ES BEI VERTRAGSGEMÄSSER NUTZUNG ODER DURCH NACHLÄSSIGKEIT ODER SONSTIGE UNERLAUBTE HANDLUNG - UND DIE DURCH ODER IM ZUSAMMENHANG MIT DER VERWENDUNG, DEM VERVIELFÄLTIGEN, MODIFIZIEREN ODER WEITERVERBREITEN DIESER SOFTWARE ENTSTANDEN SIND.

Fujitsu Ltd. and Fujitsu Technology Solutions GmbH

Der Inhalt dieses Handbuchs darf ohne die ausdrückliche, schriftliche Genehmigung von Fujitsu Limited oder Fujitsu Technology Solutions GmbH weder in irgendeiner Form weitergegeben noch mittels irgendeines Mediums reproduziert werden.

Alle Rechte vorbehalten, Copyright ©
FUJITSU LIMITED und Fujitsu Technology Solutions GmbH 2005 - 2009

U41632-J-Z816-5

Bisherige Versionen

(1/2)

Ausgabe	Datum	Überarbeiteter Abschnitt (neu/gelöscht/geändert)	Details
01	2005-07-11	—	—
02	2005-09-16	Alle Kapitel (Korrekturen) KAPITEL 3 und 4 (Korrekturen)	Technische Überarbeitung Erweiterung um die Windows-Version
03	2005-10-31	Alle Kapitel (Korrekturen)	Fehlerkorrekturen
04	2006-02-20	Alle Kapitel	Erweiterung um die Beschreibung der PRIMEQUEST 420
05	2006-04-17	KAPITEL 2 (Korrekturen) KAPITEL 2 (Korrekturen) KAPITEL 4, ANHANG E (Korrekturen)	Zusätzliche Hinweise zu Netzwerkeinstellungen Korrekturen zum Vorgehen bei der Linux-Installation Zusätzliche Hinweise bei der PSA-Installation
06	2006-08-11	Alle Kapitel (Korrekturen) KAPITEL 2 (Korrekturen) ANHANG A (Korrekturen) ANHANG D (Korrekturen)	Ergänzung der Beschreibungen für die Modelle PRIMEQUEST 500 Ergänzung der Beschreibungen für SUSE Ergänzung der Beschreibungen und Hinweise zu XPAR-Einstellungen Ergänzung der Beschreibungen von Software, die mit der PRIMEQUEST-Hardware geliefert werden Korrektur der Beschreibung zur EFI-Treiber-Einstellung Ergänzung von Hinweisen zum Austausch einer FC-Karte
07	2007-03-05	KAPITEL 4, ANHANG E (Korrektur)	Korrektur der Beschreibung der Watchdog-Einstellung
08	2007-08-31	Abschnitt 4.8 (Korrektur)	Erweiterung um die Beschreibung der Linux Dump-Funktion kdump

Hinweis: Überarbeitete Abschnitte werden in dieser Tabelle mit der jeweiligen Abschnittnummer in der aktuellen Ausgabe aufgeführt.
Abschnitte älterer Ausgaben sind mit einem Sternchen (*) markiert.

Ausgabe	Datum	Überarbeiteter Abschnitt (neu/gelöscht/geändert)	Details
09	2008-03-10	Alle Kapitel (Ergänzungen)	Ergänzung der Beschreibung für die Modelle PRIMEQUEST 580A/540A/520A
10	2008-04-10	Alle Kapitel (Korrekturen)	Technische Überarbeitung Fujitsu Technology Solutions gibt eine zusätzliche Ausgabe des Handbuchs in Deutsch heraus, passt Texte und Abbildungen an, ändert die Bestellnummer des Handbuchs, ergänzt in Handbuchverweisen die Fujitsu Technology Solutions Bestellnummern, ändert die Beschreibungen, wo PRIME-QUEST-Handbücher verfügbar sind, ergänzt Fußnoten bezüglich des Fujitsu Servicekonzepts REMCS, Speichersystems ETERNUS und Werkzeugs FST, die von Fujitsu Technology Solutions nicht unterstützt werden, ersetzt das Kommentarformular und korrigiert den Text gemäß der Korrekturtabellen (Errata) vom 2006/10/10, 2008/09/19, 2012/12/18 und 2009/02/24. **Hinweis:** **REMCS und FST werden von Fujitsu Technology Solutions nicht unterstützt.** **ETERNUS - Angebot und Support in EMEA nur für die globalen Kunden von Fujitsu.**

Hinweis: Überarbeitete Abschnitte werden in dieser Tabelle mit der jeweiligen Abschnittnummer in der aktuellen Ausgabe aufgeführt.
Abschnitte älterer Ausgaben sind mit einem Sternchen (*) markiert.

Vorwort

Dieses Handbuch beschreibt die für die Installation der PRIMEQUEST erforderlichen Vorbereitungen, die Ein- und Ausschaltsequenzen, die Initialisierungs- sowie die Softwareinstallationsverfahren. Das Handbuch ist für Systemverwalter bestimmt.

Dieser Abschnitt behandelt

- Aufbau und Inhalt des Handbuchs
- Referenzhandbücher
- Abkürzungen
- Symbolik
- Syntax des Command Line Interface (CLI)
- Hinweise zur Notation, die in diesem Handbuch verwendet wird
- Konventionen für Warnhinweise
- Umgebungsbedingungen für den Einsatz dieses Produktes
- Wichtige Hinweise/Leser-Feedback

Aufbau und Inhalt des Handbuchs

Das vorliegende Handbuch ist wie folgt aufgebaut:

KAPITEL 1 PRIMEQUEST - Überblick

Enthält einen Überblick über die Hardware, Software und Netzwerkverbindungen und beschreibt die Arbeitsabläufe, die vor der Inbetriebname erforderlich sind.

KAPITEL 2 Installation

Beschreibt die vor der Installation der Systemeinheit erforderlichen Arbeiten.

KAPITEL 3 Betriebssystem installieren

Beschreibt die unterstützten Betriebssysteme und deren Installation.

KAPITEL 4 Nach Installation des Betriebssystems erforderliche Arbeiten

Beschreibt die auf die Installation des Betriebssystems folgende Installation und Konfiguration diverser Softwareprogramme.

KAPITEL 5 Systemsicherheit

Beschreibt die SNMP- und Sicherheitseinstellungen.

KAPITEL 6 GSWB initialisieren

Beschreibt die ersten Einstellungen, die für die Benutzung des optionalen Produkts GSWB erforderlich sind.

Anhang A Zum Lieferumfang der PRIMEQUEST gehörende Software

Beschreibt die mit PRIMEQUEST zur Verfügung gestellten Softwareprogramme.

Anhang B Installation

Enthält Anweisungen zur Installation von PRIMEQUEST.

Anhang C Ein- und Ausschalten

Beschreibt, wie die Systemeinheit ein- und ausgeschaltet wird.

Anhang D SAN Boot Environment

Beschreibt, wie die SAN Boot Environment konfiguriert wird.

Anhang E Liste der Standardwerte

Enthält Listen der Default-Werte für das MMB (Server Management Board) und den PSA.

Anhang F Übersicht der IP-Adressen des Management-LANs

Beschreibt die von der PRIMEQUEST benutzten IP-Adressen.

Glossar

Erläutert wichtige Begriffe aus diesem Handbuch.

Stichwortverzeichnis

Enthält eine Liste von Schlüsselbegriffen sowie die Nummern der Seiten, auf denen diese Begriffe zu finden sind.

Referenzhandbücher

Folgende Handbücher stehen zu Referenzzwecken zur Verfügung:

a) Ausgeliefertes gedrucktes Handbuch
(ebenfalls englisch und deutsch als PDF-Datei auf http://manuals.ts.fujitsu.com/ verfügbar):

Titel	Beschreibung	Bestellnr.
PRIMEQUEST 500A/500/ 400 Series Installation Manual	Beschreibt die Installation der PRIMEQUEST einschließlich der Installationsvorbereitung, Voreinstellungen und Software-Installtion	englisch: U41632-J-Z816-x-76 (adaptiertes Fujitsu-Handbuch C122-E001EN)

b) Als PDF-Dateien auf http://manuals.ts.fujitsu.com/ (wählen Sie „Mission Critical IA Server“ aus) verfügbare Handbücher:

Titel	Beschreibung	Bestellnr.
PRIMEQUEST 580A/540A/580/ 540/480/440 System Design Guide	Enthält Anforderungen, Überlegungen und Bemerkungen zum Entwurf des Systembetriebs der PRIMEQUEST 580/540/480/440.	nur englisch: U41630-J-Z816-x-76 (adaptiertes Fujitsu-Handbuch C122-B001EN)
PRIMEQUEST 580A/540A/580/ 540/480/440 Installation Planning Manual	Enthält Spezifikationen für und Anforderungen an Aufstellungsorte, die für die Installation einer PRIMEQUEST 580/540/480/440 geeignet sind.	nur englisch: U41631-J-Z816-x-76 (adaptiertes Fujitsu-Handbuch C122-H001EN)
PRIMEQUEST 500A/500/400 Modellreihe Installationshandbuch (dieses Handbuch) *PRIMEQUEST 500/400 Series Installation Manual*	Beschreibt die Installation der PRIMEQUEST einschließlich der Installationsvorbereitung, Voreinstellungen und Software-Installation	deutsch: U41632-J-Z816-x englisch: U41632-J-Z816-x-76 (adaptiertes/übersetztes Fujitsu-Handbuch C122-E001EN)
PRIMEQUEST 520A/520/420 System Design Guide	Enthält Anforderungen, Überlegungen und Bemerkungen zum Entwurf des Systembetriebs der PRIMEQUEST 520/420.	nur englisch: U41643-J-Z816-x-76 (adaptiertes Fujitsu-Handbuch C122-B009EN)
PRIMEQUEST 520A/520/420 Installation Planning Manual	Enthält Spezifikationen für und Anforderungen an Aufstellungsorte, die für die Installation einer PRIMEQUEST 520/420 geeignet sind.	nur englisch: U41644-J-Z816-x-76 (adaptiertes Fujitsu-Handbuch C122-H002EN)

Titel	Beschreibung	Bestellnr.
PRIMEQUEST 500A/500/400 Series Reference Manual: Basic Operation/GUI/Commands	Enthält Operationen, Installationsmaßnahmen und Systemverwaltungsmethoden, die für den betrieb der PRIMEQUEST erforderlich sind. Die Erläuterungen decken grundlegende Operationen und Funktionen von MMB, PSA und EFI ab.	nur englisch: U41633-J-Z816-x-76 (adaptiertes Fujitsu-Handbuch C122-E003EN)
PRIMEQUEST 500A/500/400 Series Reference Manual: Tools/ Operation Information	Erläutert Systemverwaltung, Hot Plug, REMCS*, LEDs und weitere für den Systembetrieb erforderliche Operationen. Darüber hinaus enthält das Handbuch ergänzende Informationen z.B. über physikalische Positionen von Komponenten.	nur englisch: U41757-J-Z816-x-76 (adaptiertes Fujitsu-Handbuch C122-E074EN)
PRIMEQUEST 500A/500/400 Series Reference Manual: Messages/Logs	Erläutert Maßnahmen bei Problemen während des Betriebs und beschreibt verschiedene Typen von Meldungen.	nur englisch: U41634-J-Z816-x-76 (adaptiertes Fujitsu-Handbuch C122-E004EN)
PRIMEQUEST GSWB User's Manual	Enthält Anforderungen, wichtige Einzelheiten und Hinweise bezüglich Installation und Betrieb von GSWB, einem optionalen Produkt.	nur englisch: U41635-J-Z816-x-76 (adaptiertes Fujitsu-Handbuch C122-E028EN)
PRIMEPOWER Series/ PRIMEQUEST Series Common Installation Planning Manual	Enthält grundlegende Informationen und Strategien zur Installations- und Anlagenplanung, die für die Installation der SPARC Enterprise- und PRIMEQUEST-Serie erforderlich sind.	nur englisch: U41296-J-Z816-x-76 (adaptiertes Fujitsu-Handbuch C120-H007EN)
PRIMEQUEST 580A/540A Dynamic Partitioning (DP) Manual	Erklärt die Funktion Dynamic Partitioning (DP), die von den Modellen PRIMEQUEST 580A/540A unterstützt wird.	nur englisch: U41799-J-Z816-x-76 (adaptiertes Fujitsu-Handbuch C122-E085EN)

*: wird von Fujitsu Technology Solutions nicht unterstützt

c) Andere Handbücher, die auf
http://support.ts.fujitsu.com/com/support/downloads.html verfügbar sind
(wählen Sie „Mission Critical IA Server“ als Produkt aus)

RH Driver-CD
(die Downloads „Driver for RHEL4“ und „Driver for RHEL5“ enthalten diese Handbücher):
PRIMEQUEST Installation Support Tool User's Guide (Red Hat) (C122-E005EN)
PRIMEQUEST 480/440/420 Bundled-Software Package Installer User's Guide (C122-E006EN)
PRIMEQUEST System Parameter Check Tool User's Guide (C122-E009EN)

Suse Driver-CD
(die Downloads „Driver for SLES9“ oder „Driver for SLES10“ enthalten diese Handbücher):
PRIMEQUEST Installation Support Tool User's Guide (SUSE) (C122-E047EN)
PRIMEQUEST 480/440/420 Bundled-Software Package Installer User's Guide (C122-E006EN)

SCWL-CD
(Download „Systemcast Wizard Light CD“ enthält dieses Handbuch):
PRIMEQUEST SystemcastWizard Lite User's Guide (C122-E010EN)

Abkürzungen

In diesem Handbuch werden Produktnamen wie folgt abgekürzt:

Title	Description
Red Hat® Enterprise Linux® AS (v.4 for Itanium)	Red Hat (*1)
Red Hat® Enterprise Linux® 5 (for Intel Itanium)	
Red Hat® Enterprise Linux® AS (v.4 for Itanium)	RHEL-AS4 (IPF)
Red Hat® Enterprise Linux® 5 (for Intel Itanium)	RHEL5 (IPF) (*2)
SUSE™ Linux Enterprise Server 9 for Itanium Processor Family	SUSE
SUSE™ Linux Enterprise Server 10 for Itanium Processor Family (*)	
SUSE™ Linux Enterprise Server 9 for Itanium Processor Family	SUSE9
SUSE™ Linux Enterprise Server 10 for Itanium Processor Family	SUSE10
Microsoft® Windows® XP Professional	Windows XP
Microsoft® Windows® XP Home Edition	
Microsoft® Windows Server® 2003, Enterprise Edition for Itanium-based Systems	Windows Windows Server 2003
Microsoft® Windows Server® 2003, Datacenter Edition for Itanium-based Systems	
Microsoft® Windows Server® 2008 for Itanium-Based Systems	Windows Windows Server 2008

*1: versions-unabhängige Abkürzung

*2: Eine Abkürzung in der Form„RHEL5.x (IPF)“ steht für eine Update-Version.

Symbolik

In diesem Handbuch werden die nachfolgenden Schriften und Symbole für bestimmte Informationsarten verwendet.

Schrift/Symbole	Bedeutung	Beispiel
Kursiv	Titel eines Handbuchs.	Siehe *PRIMEQUEST 580A/540A/580/540/480/440 System Design Guide*.
„ “	Handbuch-, Kapitel- oder Abschnittstitel sowie Verweise auf bestimmte Positionen, Tasten/ Schaltflächen oder Menüs.	Siehe Kapitel 5, „Systemwartung“.
[]	Fenster, Schaltflächen, Registerblätter, Dropdown-Menüs.	Klicken Sie auf [OK], um fortzufahren.

Syntax des Command Line Interface (CLI)

Die Kommandosyntax wird im Folgenden genauer beschrieben.

Kommandosyntax

Bei der Kommandosyntax sind folgende Regeln zu beachten:

- Eine Variable, die die Eingabe eines Wertes erfordert, wird in < > eingeschlossen.
- Ein optionales Element wird in [ ] eingeschlossen.
- Eine Gruppe von Optionen für ein optionales Schlüsselwort wird in [ ] eingeschlossen. Als Trennzeichen wird | verwendet.
- Eine Gruppe von Optionen für ein obligatorisches Schlüsselwort wird in { } eingeschlossen. Als Trennzeichen wird | verwendet.

```
Die Kommandosyntax erscheint in einem Rahmen wie diesem.
```

Hinweise zur Notation, die in diesem Handbuch verwendet wird

- Eine Kennzeichnung mit „Linux“ bezieht sich auf folgende Linux-Derivate:
  Red Hat® Enterprise Linux® AS (v.4 for Itanium),
  Red Hat® Enterprise Linux® 5 (for Intel Itanium)
  SUSE™ Linux Enterprise Server 9 for Itanium Processor Family,
  SUSE™ Linux Enterprise Server 10 for Itanium Processor Family.
- Die IO Unit wird in der Bedienoberfläche des MMB und in den Abbildungen in diesem Handbuch als „IOU“ bezeichnet.

Konventionen für Warnhinweise

Im vorliegenden Handbuch werden die folgenden Konventionen für Warnhinweise verwendet. Ein Warnhinweis besteht aus einem optischen Signal und einem kurzen Text.

⚠WARNUNG	Signalisiert eine Gefahrensituation, die *schwere Verletzungen verursachen kann*, wenn der Benutzer die beschriebene Prozedur nicht korrekt ausführt.
⚠ACHTUNG	Signalisiert eine Gefahrensituation, die *leichte oder mittelschwere Verletzungen verursachen kann*, wenn der Benutzer die beschriebene Prozedur nicht korrekt ausführt. Dieses Signal weist außerdem darauf hin, dass das Produkt oder andere Gegenstände beschädigt werden *können*, wenn die Prozedur nicht korrekt ausgeführt wird.
WICHTIG	Kennzeichnet Informationen, mit deren Hilfe der Benutzer das Produkt effizienter nutzen kann.

Warnhinweis im Text

Der Hinweistext ist eingerückt, damit er leichter vom umgebenden Fließtext zu unterscheiden ist. Ferner ist er mit einem größeren Abstand vom übrigen Text abgesetzt, damit leicht erkennbar ist, wo er beginnt und endet.

⚠WARNUNG

Einige der in diesem Handbuch beschriebenen Aufgaben sollten nur von eine qualifizierten Techniker durchgeführt werden. Diese Aufgaben dürfen nicht vom Benutzer durchgeführt werden. Eine unsachgemäße Durchführung dieser Aufgaben kann zu Stromschlägen, anderen Verletzungen oder Feuergefahr führen.

- Installation und Reinstallation aller Komponenten und erste Einstellungen
- Entfernen der Front-, Seiten- oder rückwärtigen Abdeckung
- Ein-/Ausbau optionaler interner Geräte
- Einsetzen oder Herausziehen von externen Schnittstellenkarten
- Wartung und Inspektionen (Reparatur und reguläre Diagnose- und Wartungsarbeiten)

Einen Überblick über wichtige Hinweise finden Sie in der Tabelle „Wichtige Warnhinweise“ im Abschnitt „SICHERHEITSHINWEISE“, der auf dieses „Vorwort“ folgt.

Umgebungsbedingungen für den Einsatz dieses Produktes

Bei diesem Produkt handelt es sich um ein Computersystem, das für den Einsatz in einem speziellen Computerraum bestimmt ist. Weiterführende Informationen zur Betriebsumgebung finden Sie in den folgenden Handbüchern

- PRIMEQUEST 580/540/480/440 Installation Planning Manual (U41631-J-Z816-x-76/C122-H001EN)

PRIMEQUEST 520/420 Installation Planning Manual (U41644-J-Z816-x-76/C122-H002EN).

Wichtige Hinweise/Leser-Feedback

- Das Remote Customer Support System (REMCS) wird in Europa nicht unterstützt.
- Dieses Handbuch geht davon aus, dass an eine IO Unit und an ein IOX jeweils zwei BMMs (optionale Produkte) angeschlossen werden können. Dies spiegelt sich in den in diesem Handbuch enthaltenen Erklärungen und Abbildungen wider. Zum aktuellen Zeitpunkt unterstützt die PRIMEQUEST 480/440/420 Serie jedoch nur den Anschluss jeweils eines BMMs (BMM#0) je IO Unit und je IOX.
- In diesem Handbuch bedeutet der in Beschreibungen der PRIMEQUEST 480/440 verwendete Begriff BP (BackPlane) MP (MidPlane).
- Die in diesem Handbuch wiedergegebenen Bildschirme können von den auf Ihrem System tatsächlich dargestellten abweichen.
- Falls Sie irgendwelche Probleme mit der Beschreibung haben oder falls Sie inkorrekte Erklärungen finden, füllen Sie bitte das Kommentar-Formular am Ende des Handbuchs aus und schicken Sie es an die auf dem Formular angegebene Adresse.
- Der Inhalt dieses Handbuchs wird möglicherweise ohne vorherige Ankündigung überarbeitet.
- Die PDF-Version dieses Handbuchs lässt sich am besten mit dem Adobe® Reader® bei einer Vergrößerung von 100% und der Einstellung „einzelne Seite“ im Seitenlayout betrachten.

SICHERHEITSHINWEISE

Wichtige Warnhinweise

Dieses Handbuch enthält die folgenden wichtigen Warnhinweise:

⚠ ACHTUNG

Signalisiert eine Gefahrensituation, die *leichte oder mittelschwere Verletzungen verursachen kann*, wenn der Benutzer die beschriebene Prozedur nicht korrekt ausführt. Diese Signal weist außerdem darauf hin, dass das Produkt oder andere Gegenstände beschädigt werden *können*, wenn die Prozedur nicht korrekt ausgeführt wird.

Vorgang	Warnung	Seite
Normaler Betrieb	**Fehlfunktion** Das MMB Web-UI (Web User Interface) unterstützt die folgenden Browser. Andere Browser stellen das Web-UI möglicherweise nicht korrekt dar. ● Microsoft® Internet Explorer V5.5 (SP2) oder höher ● Netscape V7.02 oder höher	P.2-10
	Datenverlust Wenn der Strom zur Systemeinheit in einer Operation vom MMB abgeschaltet wird, leuchten nur die folgenden LEDs des Bedienfeldes und des MMBs: ● MMB-Ready LED des Bedienfeldes ● Power LED des MMBs ● Ready LED des MMBs ● Active LED des MMBs Stellen Sie sicher, dass alle LEDs außer diesen aus sind, bevor Sie die Hauptstromversorgung ausschalten (USV, Netzteil und Hauptnetzschalter). Ansonsten könnte das Abschalten der Hauptstromversorgung zu Datenverlust führen.	P.C-6 P.C-7
	Datenverlust Bevor Sie das System ausschalten, überprüfen Sie unbedingt Folgendes, um Datenverluste zu vermeiden: ● Es ist keine Anwendung mehr aktiv. ● Kein Benutzer greift mehr auf Systemkomponenten zu.	P.C-11

Vorgang	Warnung	Seite
Normaler Betrieb	**Fehlfunktion** Für das Ausführen der folgenden Operationen müssen Sie den Boot Watchdog auf [Disable] einstellen: ● Booten von CD-ROM ● Systemstart im Single User Mode ● Datensicherung und Datenwiederherstellung unter Verwendung des SystemcastWizard Falls diese Operationen ausgeführt werden, wenn der Boot Watchdog auf [Enable] eingestellt ist, wird der Wiederanlauf des Betriebssystems gemäß einer eingestellten Anzahl wiederholt, nachdem eine bestimmte Aktion ausgeführt wurde (Stop Reboot und Ausschalten, Stop Reboot oder Diagnostic Interrupt). Die Anzahl der Wiederanlaufsversuche und die Aktion werden im [ASR (Automatic Server Restart) Control]-Fenster des MMB eingestellt. Im [ASR (Automatic Server Restart) Control]-Fenster des MMB kann der Boot Watchdog auf [Disable] eingestellt werden, indem nach Markieren des [Cancel Boot Watchdog] [Apply] angeklickt wird.	P.4-103

Warnaufkleber

Folgende Warnaufkleber sind an diesem Produkt angebracht:

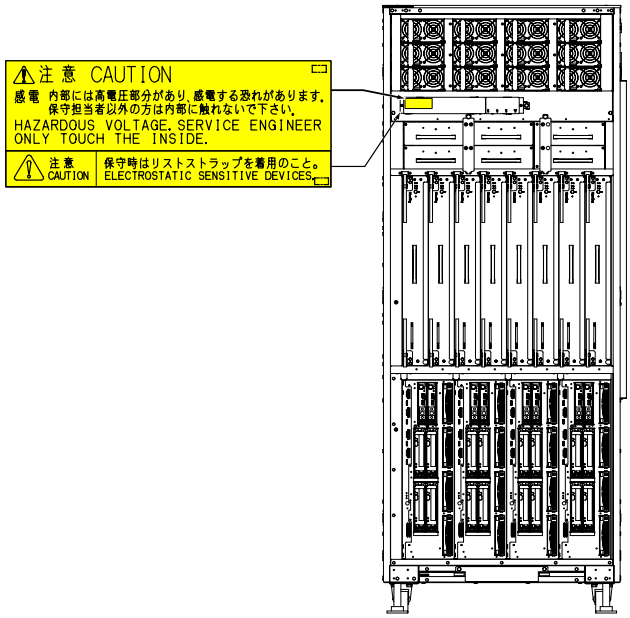
Diese Aufkleber liefern Benutzerinformationen zu dem Produkt.

⚠ ACHTUNG

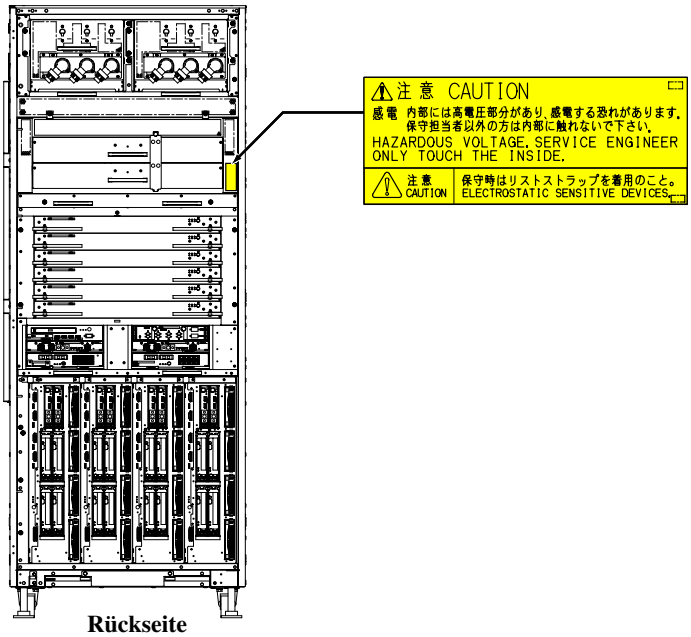
Aufkleber nicht entfernen!

PRIMEQUEST 580A/540A/580/540/480/440

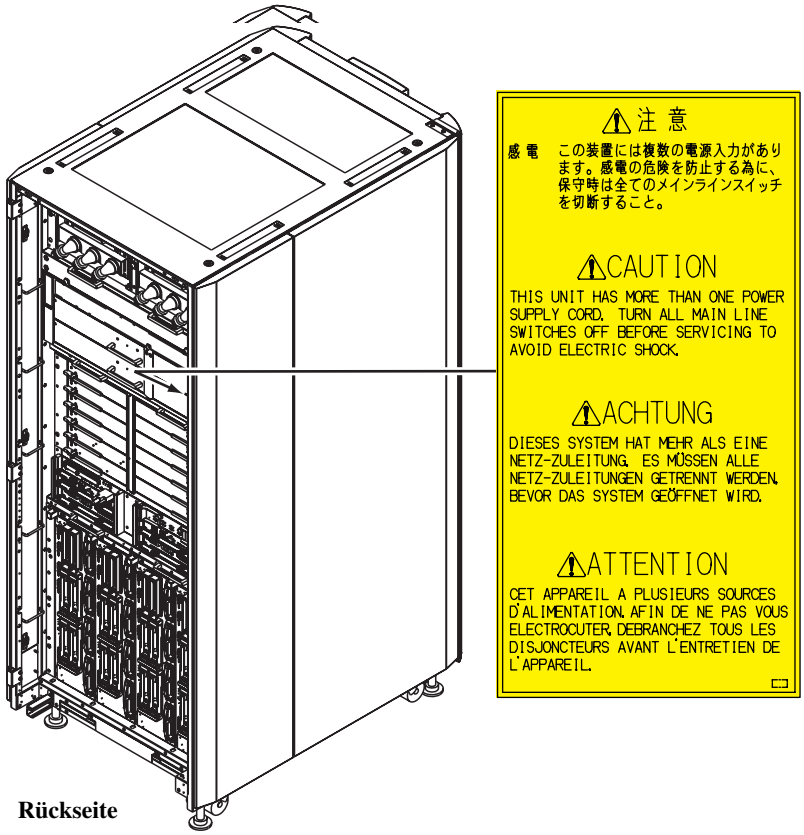
- Systemeinheit



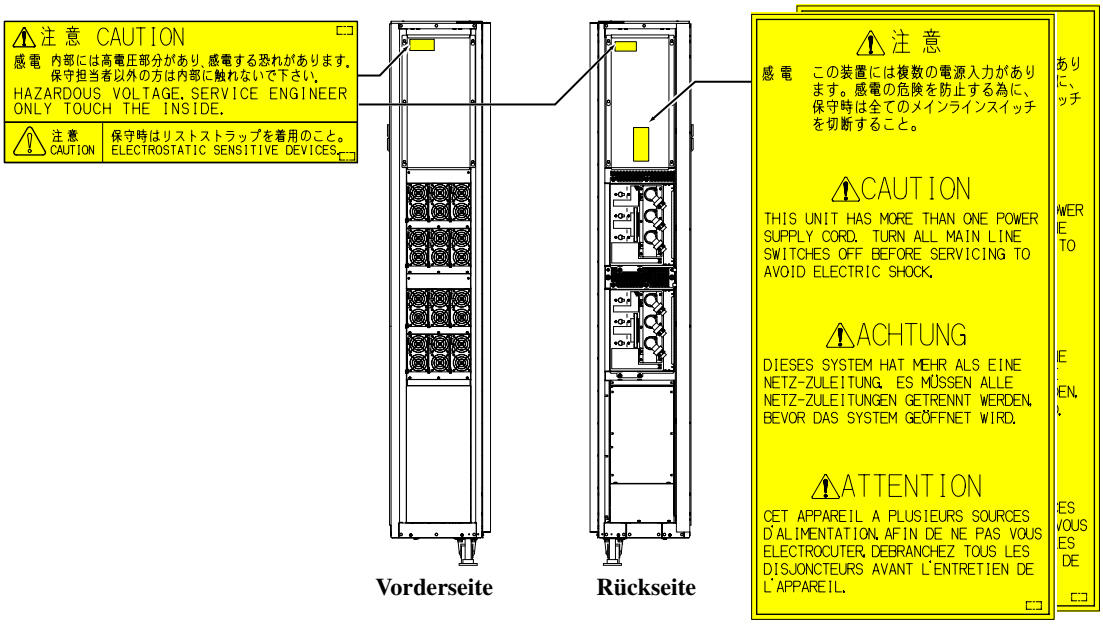
Vorderseite



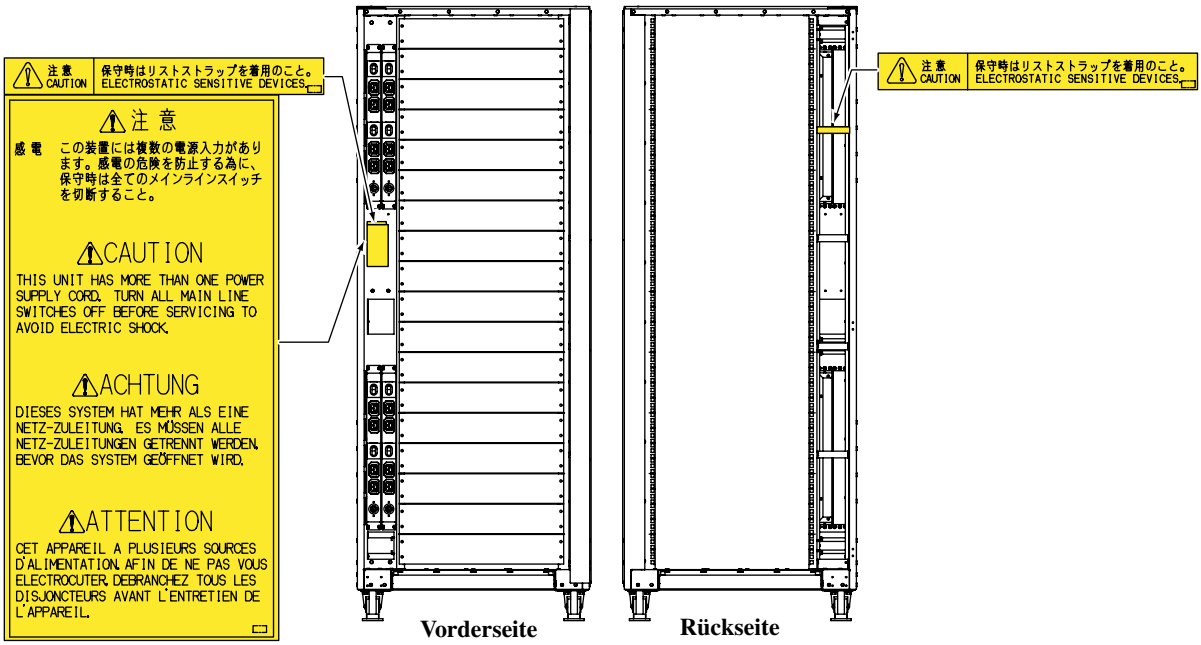
Rückseite

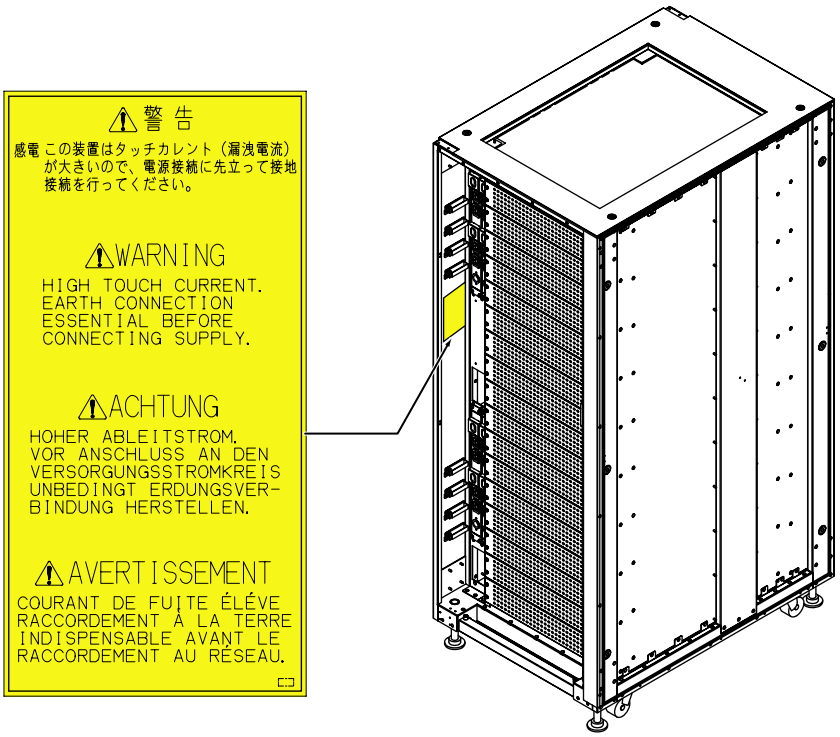

⚠注 意
感電 この装置には複数の電源入力があります。感電の危険を防止する為に、保守時は全てのメインラインスイッチを切断すること。
⚠CAUTION
THIS UNIT HAS MORE THAN ONE POWER SUPPLY CORD. TURN ALL MAIN LINE SWITCHES OFF BEFORE SERVICING TO AVOID ELECTRIC SHOCK.
⚠ACHTUNG
DIESES SYSTEM HAT MEHR ALS EINE NETZ-ZULEITUNG. ES MÜSSEN ALLE NETZ-ZULEITUNGEN GETRENNT WERDEN, BEVOR DAS SYSTEM GEÖFFNET WIRD.
⚠ATTENTION
CET APPAREIL A PLUSIEURS SOURCES D'ALIMENTATION. AFIN DE NE PAS VOUS ELECTROCUTER, DEBRANCHEZ TOUS LES DISJONCTEURS AVANT L'ENTRETIEN DE L'APPAREIL.
Rückseite

- Extended Power Cabinet (Netzteilerweiterungsschrank)

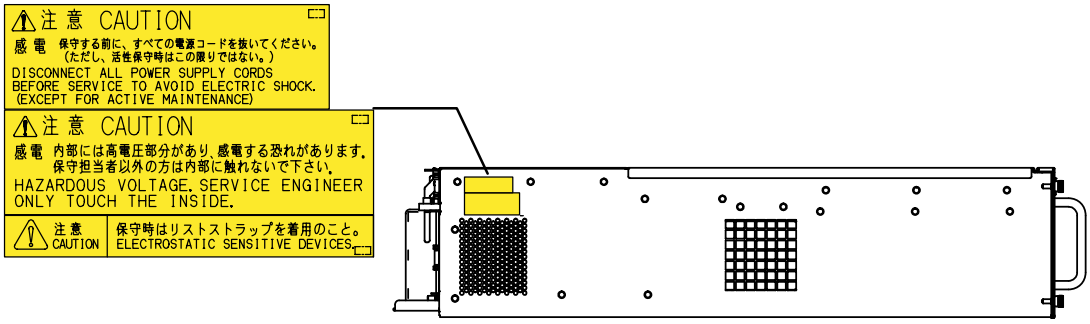

⚠注 意 CAUTION
感電 内部には高電圧部分があり、感電する恐れがあります。保守担当者以外の方は内部に触れないで下さい。
HAZARDOUS VOLTAGE. SERVICE ENGINEER ONLY TOUCH THE INSIDE.
注意 CAUTION
保守時はリストストラップを着用のこと。
ELECTROSTATIC SENSITIVE DEVICES.
⚠注 意
感電 この装置には複数の電源入力があります。感電の危険を防止する為に、保守時は全てのメインラインスイッチを切断すること。
⚠CAUTION
THIS UNIT HAS MORE THAN ONE POWER SUPPLY CORD. TURN ALL MAIN LINE SWITCHES OFF BEFORE SERVICING TO AVOID ELECTRIC SHOCK.
⚠ACHTUNG
DIESES SYSTEM HAT MEHR ALS EINE NETZ-ZULEITUNG. ES MÜSSEN ALLE NETZ-ZULEITUNGEN GETRENNT WERDEN, BEVOR DAS SYSTEM GEÖFFNET WIRD.
⚠ATTENTION
CET APPAREIL A PLUSIEURS SOURCES D'ALIMENTATION. AFIN DE NE PAS VOUS ELECTROCUTER, DEBRANCHEZ TOUS LES DISJONCTEURS AVANT L'ENTRETIEN DE L'APPAREIL.
Vorderseite
Rückseite

- Extended I/O Cabinet (E/A-Erweiterungsschrank)

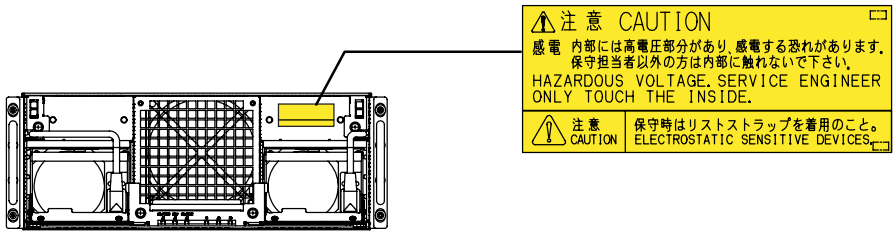

注 意 CAUTION
保守時はリストストラップを着用のこと。
ELECTROSTATIC SENSITIVE DEVICES.
注 意
感電 この装置には複数の電源入力があります。感電の危険を防止する為に、保守時は全てのメインラインスイッチを切断すること。
CAUTION
THIS UNIT HAS MORE THAN ONE POWER SUPPLY CORD. TURN ALL MAIN LINE SWITCHES OFF BEFORE SERVICING TO AVOID ELECTRIC SHOCK.
ACHTUNG
DIESES SYSTEM HAT MEHR ALS EINE NETZ-ZULEITUNG. ES MÜSSEN ALLE NETZ-ZULEITUNGEN GETRENNT WERDEN, BEVOR DAS SYSTEM GEÖFFNET WIRD.
ATTENTION
CET APPAREIL A PLUSIEURS SOURCES D'ALIMENTATION. AFIN DE NE PAS VOUS ELECTROCUTER, DEBRANCHEZ TOUS LES DISJONCTEURS AVANT L'ENTRETIEN DE L'APPAREIL.
Vorderseite
Rückseite


警 告
感電 この装置はタッチカレント（漏洩電流）が大きいので、電源接続に先立って接地接続を行ってください。
WARNING
HIGH TOUCH CURRENT. EARTH CONNECTION ESSENTIAL BEFORE CONNECTING SUPPLY.
ACHTUNG
HOHER ABLEITSTROM. VOR ANSCHLUSS AN DEN VERSORGUNGSSTROMKREIS UNBEDINGT ERDUNGSVERBINDUNG HERSTELLEN.
AVERTISSEMENT
COURANT DE FUITE ÉLÉVE RACCORDEMENT À LA TERRE INDISPENSABLE AVANT LE RACCORDEMENT AU RÉSEAU.

- PCI-Box



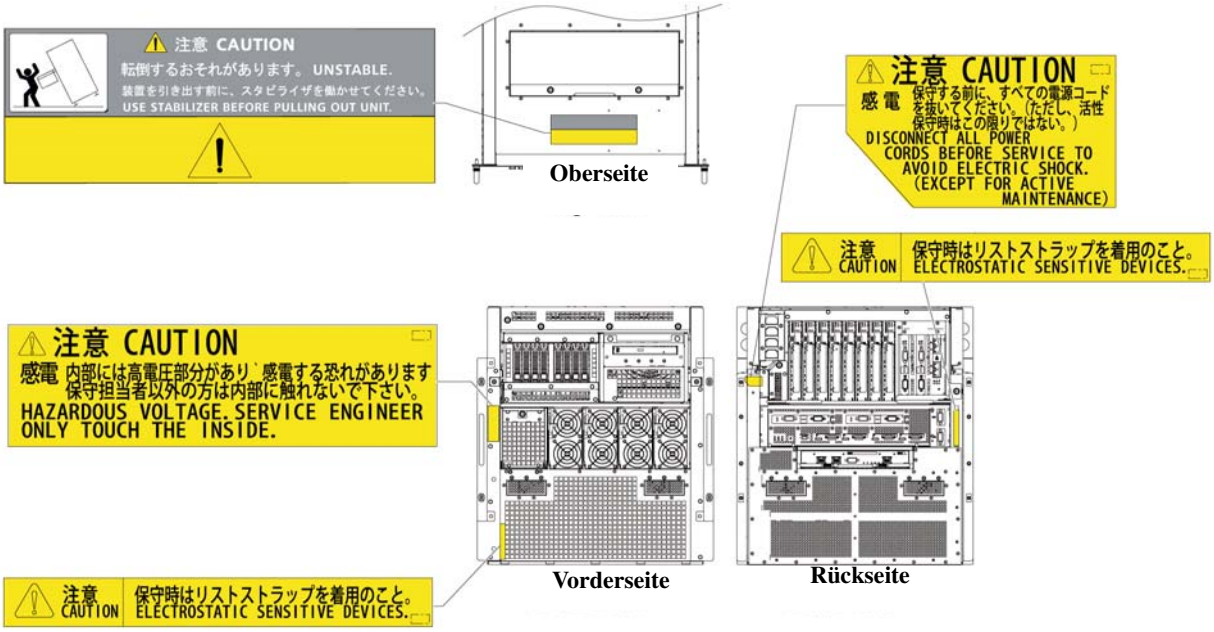
linke Seite



Vorderseite (ohne Abdeckung)

PRIMEQUEST 520A/520/420

- Systemeinheit



Umgang mit diesem Produkt

Wartung

⚠ WARNUNG

Bestimmte Wartungsmaßnahmen, die in diesem Handbuch beschrieben werden, sollten nur von qualifizierten Service-Technikern durchgeführt werden. Werden diese Maßnahmen nicht ordnungsgemäß durchgeführt, besteht Stromschlag-, Verletzungs- und Brandgefahr.

- Erstinstallation und Wiedereinbau aller Komponenten sowie alle Voreinstellungen
- Abnehmen der vorderen, hinteren und seitlichen Abdeckungen
- Ein- und Ausbau optionaler interner Geräte
- Einstecken und Abziehen externer Schnittstellenkarten
- Wartungen und Inspektionen (Reparatur sowie regelmäßige Diagnose und Wartung)

⚠ ACHTUNG

Die nachfolgenden Wartungsmaßnahmen für dieses Produkt und für die optionalen Produkte von Fujitsu oder Fujitsu Technology Solutions dürfen nur von qualifizierten Service-Technikern durchgeführt werden. Diese Maßnahmen dürfen unter keinen Umständen vom Benutzer vorgenommen werden. Werden diese Maßnahmen nicht ordnungsgemäß durchgeführt, können Fehlfunktionen auftreten.

- Auspacken optionaler Adapter und von an den Benutzer gelieferten Paketen.

Umbau/Konstruktionsänderungen

⚠ ACHTUNG

Es dürfen keine mechanischen oder elektrischen Modifikationen an dem Gerät vorgenommen werden.
Bei Einsatz dieses Gerätes nach Modifikationen oder Überholungen sind Verletzungen des Benutzers oder anderer Personen bzw. Beschädigungen von Gegenständen nicht auszuschließen.

Inhalt

Vorwort i
Aufbau und Inhalt des Handbuchs i
Referenzhandbücher iii
Abkürzungen v
Symbolik vi
Syntax des Command Line Interface (CLI) vi
Hinweise zur Notation, die in diesem Handbuch verwendet wird vi
Konventionen für Warnhinweise vii
Umgebungsbedingungen für den Einsatz dieses Produktes viii

SICHERHEITSHINWEISE ix
Wichtige Warnhinweise ix
Warnaufkleber xi

Umgang mit diesem Produkt xv
Wartung xv
Umbau/Konstruktionsänderungen xv

KAPITEL 1 PRIMEQUEST - Überblick 1-1

1.1 Arbeitsablauf für den Start des Betriebs 1-1
1.2 Installationsablauf 1-1
1.2.1 Für die Installation erforderliche Komponenten 1-3

KAPITEL 2 Installation. 2-1

2.1 Installationsvorbereitung 2-1
2.2 MMB anschließen und einrichten 2-3
2.2.1 Verbindung für den Echtbetrieb einstellen 2-3
2.2.1.1 IP-Adresse des als MMB-Konsole dienenden PCs festlegen 2-4
2.2.1.2 MMB-Konsole an den MMB-Benutzerport anschließen 2-4
2.2.1.3 Externe LAN-Verbindung der PRIMEQUEST (PRIMEQUEST 580A/540A/580/540/480/440) 2-5
2.2.1.4 Externe LAN-Verbindung der PRIMEQUEST (PRIMEQUEST 520A/520/420) 2-7
2.2.2 An- und Abmelden beim MMB und Fensterkonfiguration 2-9
2.2.2.1 An- und Abmelden bei der MMB Web-UI 2-10
2.2.2.2 Elemente des Web-UI-Fensters 2-11
2.2.3 Netzwerkeinstellungen für den Echtbetrieb 2-19
2.2.3.1 MMB-Netzwerk einrichten (PRIMEQUEST 580A/540A/580/540/480/440) 2-19
2.2.3.2 MMB-Netzwerk einrichten (PRIMEQUEST 520A/520/420) . 2-21

2.2.3.3 Telnet-Parameter einstellen 2-23
2.2.3.4 DNS-Server einrichten 2-24
2.2.3.5 SMTP-Einstellungen 2-25
2.2.4 MMB initialisieren 2-29
2.2.4.1 Benutzerkonten registrieren 2-30
2.2.4.2 Benutzerkonto für den Techniker einrichten 2-32
2.2.4.3 Systemnamen festlegen 2-33
2.2.4.4 Systemdatum und Uhrzeit einstellen 2-35
2.2.4.5 Einen Management-LAN-Hub einrichten 2-37
2.3 Extended Mirror Mode aktivieren 2-43
2.4 XPAR aktivieren (PRIMEQUEST 500A/500 Modellreihe) 2-45
2.5 Partition initialisieren 2-47
2.5.1 Reihenfolge der Einstellungen 2-47
2.5.2 Partition schließen 2-49
2.5.3 Systemboards, IO Units und IOXs teilen und wieder verbinden (nur in der Modellreihe PRIMEQUEST 500A/500) 2-51
2.5.3.1 Systemboards teilen und wieder verbinden 2-51
2.5.3.2 IO Units oder IOXs teilen und wieder verbinden 2-53
2.5.4 Partition konfigurieren 2-55
2.5.4.1 Systemboards, IO Units und IOXs hinzufügen 2-55
2.5.4.2 Systemboards, IO Units und IOXs entfernen 2-59
2.5.5 Home IO Unit festlegen 2-61
2.5.6 Systemboard reservieren 2-63
2.5.7 Partitionsnamen festlegen 2-69
2.5.8 Verschiedene Modes einstellen 2-70
2.5.9 Partition starten 2-75
2.5.10 Partitionsinformationen anzeigen 2-77
2.6 Konfiguration sichern 2-79
2.6.1 MMB-Konfigurationsdaten sichern 2-79

KAPITEL 3 Betriebssystem installieren 3-1

3.1 Überblick 3-1
3.1.1 Unterstützte Betriebssysteme 3-1
3.1.2 Installationsverfahren 3-1
3.1.3 Installationsvoraussetzungen 3-4
3.1.4 Nach Installation des Betriebssystems erforderliche Arbeiten 3-4
3.2 Installation des Betriebssystems Linux 3-6
3.2.1 Linux Installation über KVM (PRIMEQUEST 580A/540A/580/540/480/440) 3-6
3.2.1.1 Hardwarevoraussetzungen und Vorgehensweise 3-6
3.2.1.2 config-Datei für die Installation erstellen 3-7
3.2.1.3 Geräte anschließen 3-8

3.2.1.4 Linux Betriebssystem installieren 3-11
3.2.1.5 Zugehörige Softwareprogramme installieren 3-12
3.2.1.6 Nach der Installation erforderliche Aufgaben 3-12
3.2.2 Unabhängigen KVM-Switch für die Installation des Linux-Betriebssystems verwenden (PRIMEQUEST 520A/520/420) 3-13
3.2.2.1 Hardware-Voraussetzungen und Vorgehensweise 3-13
3.2.2.2 config-Datei für die Installation erstellen 3-14
3.2.2.3 Geräte anschließen 3-14
3.2.2.4 Linux Betriebssystem installieren 3-18
3.2.2.5 Zugehörige Softwareprogramme installieren 3-18
3.2.2.6 Nach der Installation erforderliche Aufgaben 3-18
3.2.3 Installation mit SystemcastWizard Lite 3-19
3.2.3.1 Hardwarevoraussetzungen und Vorgehensweise 3-19
3.2.3.2 Geräte anschließen 3-21
3.2.3.3 Linux installieren 3-23
3.2.3.4 Software-Bundle-Package installieren 3-23
3.2.3.5 Nach der Installation erforderliche Aufgaben 3-24
3.3 Windows installieren 3-25
3.3.1 Installationsvorbereitungen 3-26
3.3.1.1 SAN Boot Environment einrichten 3-26
3.3.1.2 SAN-Speichereinheit anschließen 3-27
3.3.1.3 Vor der Installation (PRIMEQUEST 580A/540A/580/540/480/440) 3-28
3.3.2 Windows mit SystemcastWizard Lite installieren 3-29
3.3.2.1 Hardwarevoraussetzungen und Vorgehensweise 3-29
3.3.2.2 Geräte anschließen 3-31
3.3.2.3 Windows installieren 3-34
3.3.3 Installation von Windows mit dem Installation Support Tool 3-34
3.3.3.1 Übersicht 3-34
3.3.3.2 Vorbereitungen 3-35
3.3.3.3 Erstellen der Installationsdiskette 3-36
3.3.3.4 Windows-Setup 3-37
3.3.4 Installation von Windows mit KVM (PRIMEQUEST 580A/540A/580/540/480/440) 3-38
3.3.4.1 Hardwarevoraussetzungen und Verfahren 3-38
3.3.4.2 Geräte anschließen 3-39
3.3.4.3 Windows installieren 3-40
3.3.4.4 Bedienerlose Installation 3-44
3.3.5 Installation von Windows mit unabhängigem KVM-Switch (PRIMEQUEST 520A/520/420) 3-49
3.3.5.1 Hardwarevoraussetzungen und Verfahren 3-49
3.3.5.2 Geräte anschließen 3-50
3.3.5.3 Windows installieren 3-51

3.3.5.4 Bedienerlose Installation 3-55
3.3.6 High Reliability Tools 3-60
3.3.6.1 Installation mit PRIMEQUEST Software Installer 3-61
3.3.6.2 Anmerkungen zum PRIMEQUEST Software Installer 3-63
3.3.7 Erforderliche Arbeiten nach der Installation 3-64
3.3.7.1 Einstellung des Bildschirmtreibers (Serie PRIMEQUEST 500A/500) 3-64
3.3.7.2 Installation des Multipath-Treibers 3-65
3.3.7.3 Plattenlaufwerk wieder einsetzen 3-65

KAPITEL 4 Nach Installation des Betriebssystems erforderliche Arbeiten 4-1

4.1 Art der erforderlichen Arbeiten 4-1
4.2 PSA installieren (Linux: Red Hat) (PRIMEQUEST 580A/540A/580/540/480/440) 4-3
4.2.1 Einstellungen des Management-LANs überprüfen 4-4
4.2.2 Einstellungen für SELinux überprüfen 4-12
4.2.3 Firewall überprüfen (Ports freigeben) 4-13
4.2.4 FJSVfefpcl installieren 4-14
4.2.5 Ziel für Partition-Traps festlegen 4-14
4.2.6 Ziel für Traps und E-Mails über MMB festlegen 4-17
4.2.7 Sonstige Einstellungen 4-18
4.2.8 PSA-Update installieren 4-20
4.2.9 SIRMS-Update installieren 4-21
4.2.10 PSA deinstallieren 4-21
4.2.11 SIRMS deinstallieren 4-22
4.3 PSA installieren (Linux: Red Hat) (PRIMEQUEST 520A/520/420) 4-23
4.3.1 Einstellungen des Management-LANs überprüfen 4-24
4.3.2 Einstellungen für SELinux überprüfen 4-27
4.3.3 Firewall überprüfen (Ports freigeben) 4-28
4.3.4 FJSVfefpcl installieren 4-29
4.3.5 Ziel für Partition-Traps festlegen 4-29
4.3.6 Ziel für Traps und E-Mails über MMB festlegen 4-33
4.3.7 Sonstige Einstellungen 4-33
4.3.8 PSA-Update installieren 4-35
4.3.9 SIRMS-Update installieren 4-36
4.3.10 PSA deinstallieren 4-36
4.3.11 SIRMS deinstallieren 4-37
4.4 PSA installieren (Linux: SUSE) (PRIMEQUEST 500A/500/400-Modellreihe) 4-38
4.4.1 Einstellungen des Management-LANs überprüfen 4-39
4.4.2 Kontrollfunktionen für syslog 4-50
4.4.3 SELinux-Funktion 4-55
4.4.4 Firewall überprüfen (Ports freigeben) 4-56

4.4.5 Ziel für Partition-Traps festlegen 4-57
4.4.6 Ziel für Traps und E-Mails über MMB festlegen 4-61
4.4.7 Sonstige Einstellungen 4-61
4.4.8 PSA-Update installieren 4-63
4.4.9 PSA deinstallieren 4-64
4.5 PSA installieren (Windows Server 2003) (PRIMEQUEST 580A/540A/580/540/480/440) 4-65
4.5.1 Einstellungen für das Management-LAN überprüfen 4-68
4.5.2 Ziel für Partition-Traps einstellen 4-75
4.5.3 Ziel für Traps und E-Mails über MMB festlegen 4-76
4.5.4 Windows-Firewall einstellen 4-77
4.5.5 Watchdog-Überwachung nach Auftreten eines Stopp-Fehlers (eines schwerwiegenden Systemfehlers) 4-78
4.5.6 PSA-Updates installieren 4-79
4.5.7 PSA deinstallieren 4-84
4.6 PSA installieren (Windows Server 2003) (PRIMEQUEST 520A/520/420) 4-85
4.6.1 Einstellungen für das Management-LAN überprüfen 4-88
4.6.2 Ziel für Partition-Traps einstellen 4-89
4.6.3 Ziel für Traps und E-Mails über MMB festlegen 4-91
4.6.4 Windows-Firewall einstellen 4-91
4.6.5 Watchdog-Überwachung nach Auftreten eines Stopp-Fehlers (eines schwerwiegenden Systemfehlers) 4-93
4.6.6 PSA-Updates installieren 4-94
4.6.7 PSA deinstallieren 4-98
4.7 PSA-Einstellungen 4-99
4.8 PSA-Überwachung konfigurieren 4-99
4.8.1 S.M.A.R.T. einrichten 4-99
4.8.2 Watchdog einrichten nach Auftreten eines Stopp-Fehlers 4-101
4.9 Dump-Umgebung einrichten (Linux: Red Hat) 4-107
4.9.1 Dump-Umgebung einrichten 4-110
4.9.1.1 Dump Device anlegen 4-110
4.9.1.2 Dump-Speicherbereich zuweisen 4-112
4.9.2 diskdump einrichten 4-114
4.9.3 kdump einrichten 4-119
4.9.3.1 kexec-Tools installieren 4-120
4.9.3.2 Vergeben eines Labels für den Dump-Speicherbereich 4-121
4.9.3.3 Dump-Umgebung einrichten 4-121
4.9.3.4 kdump-Dienst einrichten 4-122
4.9.3.5 Kernel-Parameter setzen 4-122
4.9.3.6 System neu starten 4-122
4.9.3.7 kdump-Erstellung überprüfen 4-123

4.10 Dump-Umgebung einrichten (Windows Server 2003) 4-125
4.10.1 Memory Dump- und Paging-Datei einrichten 4-125
4.10.1.1 Art der Informationen, die aus einem Memory Dump gewonnen werden können 4-125
4.10.1.2 Einstellen des Memory Dump 4-127
4.10.1.3 Überprüfen der Memory Dump-Einstellungen 4-129
4.10.1.4 Paging-Datei einrichten 4-129
4.10.1.5 Hinweis 4-132
4.10.2 Präventive Fehlerbehebung mit [DSNAP] 4-133
4.11 NTP-Client einrichten 4-134
4.11.1 NTP-Betrieb bei PRIMEQUEST 4-134
4.11.2 NTP-Server einrichten 4-136
4.11.3 Partitionen als NTP-Clients einrichten 4-137
4.11.3.1 NTP-Clientbetrieb in einer Linux-Partition 4-137
4.11.3.2 NTP in einer Windows-Partition einrichten 4-138
4.11.3.3 NTP-Einstellung für eine Partition, die zu einer Domain gehört 4-141
4.12 Betriebssystem sichern 4-142
4.12.1 Linux (Red Hat) sichern 4-142
4.12.1.1 Sicherung ohne PRIMECLUSTER GDS 4-143
4.12.1.2 Datensicherung mit PRIMECLUSTER GDS 4-150
4.12.2 Windows-Partitionen sichern 4-150
4.13 Konfigurationsdaten sichern 4-151
4.13.1 PSA-Konfigurationsdaten sichern 4-151
4.13.1.1 Exportierte Dateien auflisten 4-151
4.13.1.2 In eine CSV-Datei sichern 4-153
4.13.2 EFI-Konfigurationsdaten sichern 4-154

KAPITEL 5 Systemsicherheit 5-1

5.1 Sicherheitseinstellungen 5-1
5.1.1 Zugriffskontrolle einstellen 5-2
5.1.2 SNMP einrichten 5-5
5.1.3 SSH-Parameter festlegen 5-13
5.1.4 HTTPS-Parameter festlegen 5-14

KAPITEL 6 GSWB initialisieren 6-1

Anhang A Zum Lieferumfang der PRIMEQUEST gehörende Software . . A-1

A.1 Software-Kategorien A-3
A.2 Installation Support Tool A-4
A.3 Bundled-Software Package Installer A-4
A.4 DSNAP A-5
A.5 System Parameter Check Tool A-5

A.6 System Data Output Tool (fjsnap) A-6
A.7 SystemcastWizard Lite A-7
A.7.1 SystemcastWizard Lite im Überblick A-7
A.7.2 SystemcastWizard Lite konfigurieren A-8
A.7.3 SystemcastWizard Lite installieren A-8
A.7.4 SystemcastWizard Lite benutzen A-9
A.7.5 Zur Beachtung A-10
A.8 Installation Support Tool für Windows A-11
A.9 Software Support Guide A-11

Anhang B Installation B-1

B.1 Anschluss eines PCs B-1
B.2 MMB initialisieren B-4
B.3 Anmelden beim Web-UI B-5

Anhang C Ein- und Ausschalten C-1

C.1 Ein- und Ausschalten der Systemeinheit C-1
C.1.1 Betätigung der Schutzschalter C-1
C.1.1.1 Einschalten des Systems über die Schutzschalter (PRIMEQUEST 580A/540A/580/540/480/440) C-2
C.1.1.2 System einschalten (PRIMEQUEST 520A/520/420) C-5
C.1.1.3 System über die Schutzschalter ausschalten (PRIMEQUEST 580A/540A/580/480/480/440) C-6
C.1.1.4 System ausschalten (PRIMEQUEST 520A/520/420) C-7
C.1.2 Ein- und Ausschalten des gesamten Systems C-8
C.1.2.1 Gesamtes System einschalten C-8
C.1.2.2 Gesamtes System ausschalten C-11
C.2 Schränke und Partitionen ein- und ausschalten C-13
C.3 Partitionen ein- und ausschalten C-15
C.3.1 Partition einschalten C-15
C.3.2 Partition ausschalten C-20

Anhang D SAN Boot Environment D-1

D.1 Voraussetzungen D-1
D.2 SAN Boot Environment einrichten D-2
D.3 Planung D-2
D.3.1 Planungshinweise D-4
D.4 Einstellungen D-6
D.4.1 Bereiche reservieren (RAID-Gruppen, logische Einheiten) D-6
D.4.2 Einstellungen für logische Einheiten vornehmen D-6
D.4.3 FC-Switch einrichten D-7
D.4.4 EFI-Treiber konfigurieren D-8

D.4.4.1 EFI-Treiber (Version 3.10a6) konfigurieren D-8
D.4.4.2 EFI-Treiber (Version 3.11a4/ Version 3.11x1 konfigurieren) . D-13
D.4.5 Hinweise zum Austausch eine FC-Karte D-18
D.5 Installation des Betriebssystems D-19

Anhang E Liste der Standardwerte E-1

E.1 Default-Werte für MMB E-1
E.2 Werte für PSA eingeben E-15

Anhang F Übersicht der IP-Adressen des Management-LANs F-1

Glossar GL-1

Stichwortverzeichnis IN-1

Abbildungen

Abbildung 1.1 Installationsablauf 1-2
Abbildung 2.1 Position des MMB-Benutzerports 2-4
Abbildung 2.2 Management-LANs und IP-Adressen konfigurieren (PRIMEQUEST 580A/540A/580/540/480/440) 2-5
Abbildung 2.3 Management-LANs und IP-Adressen konfigurieren (PRIMEQUEST 520/420) 2-7
Abbildung 2.4 Aufbau des Fensters [Web-UI Frame Information] 2-11
Abbildung 2.5 Untermenü 2-14
Abbildung 2.6 Aufbau des rechten Teilfensters 2-15
Abbildung 2.7 Fenster [Network Interface] (PRIMEQUEST 580A/540A/580/540/480/440) 2-20
Abbildung 2.8 Das Fenster [Network Interface] (PRIMEQUEST 520A/520/420) 2-22
Abbildung 2.9 Das Fenster [Network Protocols] 2-23
Abbildung 2.10 Fenster [Network Interface] (PRIMEQUEST 580A/540A/580/540/480/440) 2-24
Abbildung 2.11 Das Fenster [Network Interface] (PRIMEQUEST 520A/520/420) 2-25
Abbildung 2.12 Das Fenster [Alarm E-Mail] 2-26
Abbildung 2.13 Das Fenster [Alarm E-Mail Filtering Condition] (PRIMEQUEST 580A/540A/580/540/480/440) 2-28
Abbildung 2.14 Das Fenster [Alarm E-Mail Filtering Condition] (PRIMEQUEST 520A/520/420) 2-28
Abbildung 2.15 Das Fenster [User List] 2-30
Abbildung 2.16 Das Fenster [Add User] 2-31
Abbildung 2.17 Das Fenster [System Information] 2-33
Abbildung 2.18 Das Fenster [Date/Time] 2-35
Abbildung 2.19 Das Fenster [Management LAN Port Configuration] (PRIMEQUEST 580A/540A/580/540/480/440) 2-41
Abbildung 2.20 Das Fenster [Management LAN Port Configuration] (PRIMEQUEST 520A/520/420) 2-41
Abbildung 2.21 Das Fenster [Mirror License] 2-43
Abbildung 2.22 Fenster [XPAR License] 2-45
Abbildung 2.23 Das Fenster [Power Control] 2-49
Abbildung 2.24 Fenster [SB Split] 2-52
Abbildung 2.25 Fenster [IOU Split] (PRIMEQUEST 580A/540A/580/540) . . . 2-53
Abbildung 2.26 Fenster [IOU Split] (PRIMEQUEST 520A/520) 2-53
Abbildung 2.27 Das Fenster [Partition Configuration] (PRIMEQUEST 580A/540A/580/540/480/440) 2-56

Abbildung 2.28 Das Fenster [Partition Configuration] (PRIMEQUEST 520A/520/420) 2-56
Abbildung 2.29 Das Fenster [Add SB/IOU to Partition] 2-58
Abbildung 2.30 Das Fenster [Partition Configuration] (PRIMEQUEST 580A/540A/580/540/480/440) 2-59
Abbildung 2.31 Das Fenster [Partition Configuration] (PRIMEQUEST 520A/520/420) 2-60
Abbildung 2.32 Das Fenster [Remove SB/IOU from Partition] 2-60
Abbildung 2.33 Das Fenster [Partition Configuration] (PRIMEQUEST 580A/540A/580/540/480/440) 2-62
Abbildung 2.34 Das Fenster [Partition Configuration] (PRIMEQUEST 520A/520/420) 2-62
Abbildung 2.35 Das Fenster [Partition Home] 2-63
Abbildung 2.36 Das Fenster [Reserved SB Configuration] (PRIMEQUEST 580A/540A und PRIMEQUEST 580/540: Anzeige bei MMB-Firmwareversion 3.24 oder später) 2-65
Abbildung 2.37 Das Fenster [Reserved SB Configuration] (PRIMEQUEST 580/540: Anzeige bei MMB-Firmwareversion 3.23 oder früher.) 2-66
Abbildung 2.38 Das Fenster [Reserved SB Configuration] (PRIMEQUEST 480/440) 2-66
Abbildung 2.39 Das Fenster [Reserved SB Configuration] (PRIMEQUEST 520A und PRIMEQUEST 520: Anzeige bei MMB-Firmwareversion 3.24 oder später.) 2-67
Abbildung 2.40 Das Fenster [Reserved SB Configuration] (PRIMEQUEST 520: Anzeige bei MMB-Firmwareversion 3.23 oder früher) 2-67
Abbildung 2.41 Das Fenster [Reserved SB Configuration] (PRIMEQUEST 420) 2-68
Abbildung 2.42 Das Fenster [Partition Configuration] (PRIMEQUEST 580A/540A/580/540/480/440) 2-69
Abbildung 2.43 Das Fenster [Partition Configuration] (PRIMEQUEST 520A/520/420) 2-69
Abbildung 2.44 Das Fenster [Mode] (PRIMEQUEST 580A/540A) 2-71
Abbildung 2.45 Das Fenster [Mode] (PRIMEQUEST 580/540) 2-71
Abbildung 2.46 Das Fenster [Mode] (PRIMEQUEST 520A/520) 2-71
Abbildung 2.47 Das Fenster [Mode] (PRIMEQUEST 480/440) 2-72
Abbildung 2.48 Das Fenster [Mode] (PRIMEQUEST 420) 2-72
Abbildung 2.49 Das Fenster [Power Control] 2-75
Abbildung 2.50 Das Fenster [Information] 2-77
Abbildung 2.51 Das Fenster [Backup MMB Configuration] 2-79

Abbildung 3.1 Anschlüsse für eine Installation über KVM 3-8
Abbildung 3.2 Das Fenster [USB/Video/DVD Switch] 3-8
Abbildung 3.3 Das Fenster [Boot Control] 3-9
Abbildung 3.4 Fenster [Mode] (PRIMEQUEST 580A/540A) 3-10
Abbildung 3.5 Das Fenster [Power Control] 3-11
Abbildung 3.6 Anschlüsse für eine Installation über unabhängigen KVM-Switch 3-15
Abbildung 3.7 Das Fenster [DVD Switch] 3-15
Abbildung 3.8 Das Fenster [Boot Control] 3-16
Abbildung 3.9 Das Fenster [Power Control] 3-17
Abbildung 3.10 Anschlussbeispiel für die Installation mit SystemcastWizard Lite 3-21
Abbildung 3.11 Das Fenster [Remote Server Management] (Beispiel) 3-22
Abbildung 3.12 Das Fenster [Edit User] (Beispiel) 3-22
Abbildung 3.13 Arbeitsschritte für den Start des Systembetriebs 3-25
Abbildung 3.14 Das Fenster [Mode] (PRIMEQUEST 580A/540A) 3-28
Abbildung 3.15 Anforderungen für die Installation mit SystemcastWizard Lite (Windows) 3-31
Abbildung 3.16 Das Fenster [Remote Server Management] 3-32
Abbildung 3.17 Das Fenster [Edit User] 3-33
Abbildung 3.18 Anschlüsse für eine Installation mit KVM 3-39
Abbildung 3.19 Das Fenster [USB/Video/DVD Switch] 3-39
Abbildung 3.20 Fenster [Power Control] 3-40
Abbildung 3.21 Tera Term-Startfenster 3-46
Abbildung 3.22 Setup-Fenster 3-46
Abbildung 3.23 Zustimmung zur Software-Lizenz 3-47
Abbildung 3.24 Eingabe des Produktschlüssels 3-47
Abbildung 3.25 Neustart des Betriebssystems 3-48
Abbildung 3.26 Installation mithilfe des unabhängigen KVM-Switches 3-50
Abbildung 3.27 Das Fenster [DVD Switch] 3-50
Abbildung 3.28 Das Fenster [Power Control] 3-51
Abbildung 3.29 Tera Term-Startfenster 3-58
Abbildung 3.30 Setup-Fenster 3-58
Abbildung 3.31 Zustimmung zur Software-Lizenz 3-59
Abbildung 3.32 Eingabe der Produktkennung 3-59
Abbildung 3.33 Neustart des Betriebssystems 3-60
Abbildung 3.34 High-Reliability Tools Installer: Startfenster 3-61
Abbildung 4.1 Konzept eines redundanten PRIMEQUEST-Management-LANs 4-7
Abbildung 4.2 Konzept eines redundanten PRIMEQUEST-Management-LANs (Konfiguration mit erhöhter Verfügbarkeit) 4-7

Abbildung 4.3 Konzept eines redundanten PRIMEQUEST-Management-LANs 4-43
Abbildung 4.4 Konzept eines redundanten PRIMEQUEST-Management-LANs (Konfiguration mit erhöhter Verfügbarkeit) 4-43
Abbildung 4.5 Duplizierung des Management-LAN bei PRIMEQUEST 4-46
Abbildung 4.6 Duplizierung des Management-LAN bei PRIMEQUEST (Konfiguration mit verbesserter Zuverlässigkeit) 4-46
Abbildung 4.7 YaST-Fenster 4-49
Abbildung 4.8 Yast Startbildschirm 4-51
Abbildung 4.9 Bildschirm Novell AppArmor-select 4-51
Abbildung 4.10 Bildschirm AppArmor Profile select 4-52
Abbildung 4.11 Bildschirm Entry addition and selection 4-53
Abbildung 4.12 Bildschirm Adding the Profiles Entry 4-54
Abbildung 4.13 Bildschirm Entry list 4-54
Abbildung 4.14 Bildschirm Saving the profiles 4-55
Abbildung 4.15 Fenster [Computer Management] 4-70
Abbildung 4.16 Registerblatt [Teaming] 4-71
Abbildung 4.17 Dialogfenster [New Team Wizard] 4-71
Abbildung 4.18 Liste der Netzwerkadapter 4-72
Abbildung 4.19 Team-Modus-Liste 4-72
Abbildung 4.20 Auswahl abgeschlossen 4-73
Abbildung 4.21 Eigenschaften des Teams Nummer 0 4-73
Abbildung 4.22 Dialogfenster [Local Area Connection Properties] 4-74
Abbildung 4.23 Registerblatt [Advanced] 4-75
Abbildung 4.24 Dialogfenster [Add a Port] 4-77
Abbildung 4.25 Dilaogfenster [Add a Port] 4-78
Abbildung 4.26 Installationsvorbereitung 4-80
Abbildung 4.27 Update-Installation 4-80
Abbildung 4.28 Update abgeschlossen 4-81
Abbildung 4.29 Installationsvorbereitung 4-81
Abbildung 4.30 [Detected previous version of PSA] 4-82
Abbildung 4.31 Update-Installation 4-82
Abbildung 4.32 Fenster [Select Features] 4-83
Abbildung 4.33 Installation abgeschlossen 4-83
Abbildung 4.34 Bestätigungsfenster 4-84
Abbildung 4.35 Deinstallation abgeschlossen 4-84
Abbildung 4.36 Dialogfenster [Add a Port] 4-92
Abbildung 4.37 Dialogfenster [Add a Port] 4-92
Abbildung 4.38 Installationsvorbereitung 4-94
Abbildung 4.39 Update-Installation 4-94
Abbildung 4.40 Update abgeschlossen 4-95

Abbildung 4.41 Installationsvorbereitung 4-95
Abbildung 4.42 [Detected previous version of PSA] 4-96
Abbildung 4.43 Update-Installation 4-96
Abbildung 4.44 Fenster [Select Features] 4-97
Abbildung 4.45 Installation abgeschlossen 4-97
Abbildung 4.46 Bestätigungsfenster 4-98
Abbildung 4.47 Deinstallation abgeschlossen 4-98
Abbildung 4.48 Das Fenster [S.M.A.R.T.] 4-101
Abbildung 4.49 [Power Control]-Fenster 4-102
Abbildung 4.50 Das Fenster [Watchdog] 4-104
Abbildung 4.51 RHEL-AS4 (IPF) Dump-Umgebung 4-107
Abbildung 4.52 RHEL5 (IPF) Dump-Umgebung 4-108
Abbildung 4.53 Das Dialogfeld [Startup and Recovery] 4-128
Abbildung 4.54 Das Dialogfeld [Performance Options] 4-130
Abbildung 4.55 Das Dialogfeld [Virtual Memory] 4-131
Abbildung 4.56 Bestätigungsfenster 4-132
Abbildung 4.57 Konfiguration bei Nutzung externer NTP-Server 4-135
Abbildung 4.58 Das Fenster [Date/Time] (Beispiel) 4-136
Abbildung 4.59 Einstellen der IP-Adresse des NTP-Servers (Beispiel) 4-137
Abbildung 4.60 Virtuelle IP-Adresse des MMB einstellen (Beispiel) 4-139
Abbildung 4.61 Dialogbox [Date and Time Properties] (bei Zeitsynchronisation mit einem NTP-Server) 4-141
Abbildung 4.62 Das Fenster [Export List] (Beispiel) 4-152
Abbildung 4.63 Das Fenster [Export] (Beispiel) 4-154
Abbildung 4.64 Das Fenster [Backup EFI Configuration] (Beispiel) 4-154
Abbildung 5.1 Das Fenster [Access Control] (Beispiel) 5-2
Abbildung 5.2 Das Fenster [Edit Filter] (Beispiel) 5-3
Abbildung 5.3 Das Fenster [Network Protocols] (Beispiel) 5-5
Abbildung 5.4 Das Fenster [SNMP Community] (Beispiel) 5-6
Abbildung 5.5 Das Fenster [SNMP Trap] (Beispiel) 5-9
Abbildung 5.6 Das Fenster [SNMP v3 Configuration] (Beispiel) 5-11
Abbildung 5.7 Das Fenster [Network Protocols] (Beispiel) 5-13
Abbildung 5.8 Das Fenster [Network Protocols] (Beispiel) 5-15
Abbildung A.1 Sammeln von Systemdaten mit fjsnap A-6
Abbildung A.2 Konfiguration der Bundled-Version von SystemcastWizard Lite A-8
Abbildung A.3 Installationskonsole starten A-9
Abbildung B.4 Position des MMBs und der externen Schnittstellen B-2
Abbildung B.5 Das Fenster [Web-UI Frame Information] B-6
Abbildung C.1 Position der Schutzschalter (Basisschrank) C-2
Abbildung C.2 Position der Schutzschalter (Extended Power Cabinet) C-3
Abbildung C.3 Position der Schutzschalter (Extended I/O Cabinet) C-4

Abbildung C.4 Position des ACS C-5
Abbildung C.5 Das Fenster [System Power Control] C-9
Abbildung C.6 Das Fenster [System Power Control] C-12
Abbildung C.7 Das Fenster [System Power Control] C-13
Abbildung C.8 Das Fenster [Power Control] C-15
Abbildung C.9 Das Fenster [Power Control] C-20
Abbildung D.10 Beispiel für eine SAN 2-Wege-Konfiguration D-3
Abbildung D.11 Beispiel für eine SAN 4-Wege-Konfiguration D-3
Abbildung F.1 Netzwerkkonfiguration und IP-Adressen des Management-LANs (PRIMEQUEST 580A/540A/580/540/480/440) F-1
Abbildung F.2 Netzwerkkonfiguration und IP-Adressen des Management-LANs (PRIMEQUEST 52A/520/420) F-3

Tabellen

Tabelle 2.1 Systemstatus-Anzeige 2-12
Tabelle 2.2 Status anzeige 2-16
Tabelle 2.3 Feldnamen und mögliche Eingaben im Fenster [Network Interface] 2-20
Tabelle 2.4 Feldnamen und mögliche Eingaben im Fenster [Network Interface] 2-21
Tabelle 2.5 Feldnamen und mögliche Eingaben im Fenster [Network Interface] 2-22
Tabelle 2.6 Feldnamen und mögliche Eingaben im Fenster [Network Interface] 2-23
Tabelle 2.7 Feldnamen und mögliche Eingaben im Fenster [Network Interface] 2-25
Tabelle 2.8 Feldnamen und mögliche Eingaben im Fenster [Alarm E-Mail] . 2-26
Tabelle 2.9 Feldnamen und mögliche Eingaben im Fenster [Alarm E-mail Filtering Condition] 2-29
Tabelle 2.10 Feldnamen und mögliche Eingaben im Fenster [User List] 2-30
Tabelle 2.11 Feldnamen und mögliche Eingaben im Fenster [Add User] 2-31
Tabelle 2.12 Feldnamen und mögliche Eingaben im Fenster [System Information]. 2-34
Tabelle 2.13 Feldnamen und mögliche Eingaben im Fenster [Date/Time] . . . 2-36
Tabelle 2.14 Aktivierte Ports in einem Management-LAN ohne VLAN-Modus 2-39
Tabelle 2.15 Aktivierte Ports in einem Management-LAN mit VLAN-Modus 1 2-39
Tabelle 2.16 Aktivierte Ports in einem Management-LAN im Port Disable-Modus 2-40
Tabelle 2.17 Feldnamen und mögliche Eingaben im Fenster [Management LAN Port Configuration]. 2-42
Tabelle 2.18 Feldnamen und mögliche Eingaben im Fenster [Mirror License] 2-44
Tabelle 2.19 Feldnamen und mögliche Eingaben im Fenster [XPAR License] 2-46
Tabelle 2.20 Feldnamen und mögliche Eingaben im Fenster [Power Control] 2-50
Tabelle 2.21 Feldnamen und mögliche Eingaben im Fenster [SB Split]. 2-52
Tabelle 2.22 Feldnamen und mögliche Eingaben im Fenster [IOU Split] 2-54
Tabelle 2.23 Feldnamen und mögliche Eingaben im Fenster [Partition Configuration] 2-57
Tabelle 2.24 Feldnamen und mögliche Eingaben im Fenster [Add SB/IOU to Partition] 2-58
Tabelle 2.25 Feldnamen und mögliche Eingaben im Fenster [Remove SB/IOU from Partition] 2-61
Tabelle 2.26 Feldnamen und mögliche Eingaben im Fenster [Partition Home] 2-63

Tabelle 2.27	Feldnamen und mögliche Eingaben im Fenster [Mode]	2-73
Tabelle 2.28	Feldnamen und mögliche Eingaben im Fenster [Power Control]	2-76
Tabelle 2.29	Feldnamen und mögliche Eingaben im Fenster [Information]	2-77
Tabelle 3.1	Vergleich der Installationsverfahren für Linux	3-2
Tabelle 3.2	Vergleich der Installationsverfahren für Windows	3-3
Tabelle 3.3	Aufgaben nach der Installation	3-5
Tabelle 3.4	Voraussetzungen für das Installation Support Tool	3-6
Tabelle 3.5	Systemvoraussetzungen des Installation Support Tools	3-13
Tabelle 3.6	Systemvoraussetzungen im Überblick	3-19
Tabelle 3.7	Systemvoraussetzungen im Überblick	3-29
Tabelle 3.8	Systemvoraussetzungen für das Installation Support Tool for Windows	3-36
Tabelle 3.9	Produktkennungen	3-43
Tabelle 3.10	Terminalsoftware-Einstellungen	3-45
Tabelle 3.11	Produktkennungen	3-55
Tabelle 3.12	Terminalsoftware-Einstellungen	3-57
Tabelle 3.13	Von PRIMEQUEST Software Installer installierte Tools und Treiber	3-62
Tabelle 4.1	Erforderliche Aufgaben	4-1
Tabelle 4.2	Sicherheitsstufen	4-16
Tabelle 4.3	Sicherheitsstufen	4-31
Tabelle 4.4	Sicherheitsstufen	4-58
Tabelle 4.5	Ein- und Ausgabe von Daten im Fenster [Watchdog]	4-105
Tabelle 4.6	Als Dump Device einsetzbare Geräte	4-112
Tabelle 4.7	Art und Größe des Dumps	4-126
Tabelle 4.8	Elemente des [Export]-Fensters	4-153
Tabelle 5.1	Ein- und Ausgabe von Daten im Fenster [Access Control]	5-2
Tabelle 5.2	Ein- und Ausgabe von Daten im Fenster [Edit Filter]	5-4
Tabelle 5.3	Ein- und Ausgabe von Daten im Fenster [Network Protocols]	5-6
Tabelle 5.4	Ein- und Ausgabe von Daten im Fenster [SNMP Community]	5-7
Tabelle 5.5	Ein- und Ausgabe von Daten im Fenster [SNMP Trap]	5-9
Tabelle 5.6	Ein- und Ausgabe von Daten im Fenster [SNMP v3 Configuration]	5-12
Tabelle 5.7	Einstellungen für SSH	5-14
Tabelle 5.8	Einstellungen für HTTPS	5-15
Tabelle A.1	Liste der Software-Programme, die mit der PRIMEQUEST-Hardware geliefert werden	A-1
Tabelle A.2	Informationen, die die Tools des Software Support Guide liefern	A-11
Tabelle B.3	Externe Schnittstellen des MMBs	B-3
Tabelle B.4	Einstellungen der Terminalsoftware	B-3

Tabelle C.1 Ein- und Ausgabe von Daten im Fenster [System Power Control] C-10
Tabelle C.2 Ein- und Ausgabe von Daten im Fenster [System Power Control] C-14
Tabelle C.3 Ein- und Ausgabe von Daten im Fenster [Power Control] C-16
Tabelle E.1 Liste der möglichen Werte für MMB E-1
Tabelle E.2 Liste der möglichen Werte für PSA E-15

KAPITEL 1 PRIMEQUEST - Überblick

1.1 Arbeitsablauf für den Start des Betriebs

Dieser Abschnitt beschreibt den Arbeitsablauf, der für den Start des PRIMEQUEST-Betriebs erforderlich ist.
Einen Überblick über die Hardware und Software finden Sie in folgenden Handbüchern:

- PRIMEQUEST 580A/540A/580/540/480/440
  PRIMEQUEST 580A/540A/580/540/480/440 System Design Guide
  (U41630-J-Z816-x-76/C122-B001EN).
- PRIMEQUEST 520A/520/420
  PRIMEQUEST 520A/520/420 System Design Guide
  (U41643-J-Z816-x-76/C122-B009EN).

1.2 Installationsablauf

Dieser Abschnitt beschreibt die Installation der PRIMEQUEST. Einige Arbeiten sollten von qualifizierten Service-Technikern ausgeführt werden, andere vom Benutzer des Systems. Dieser Abschnitt deckt die Arbeiten ab, die vom Benutzer ausgeführt werden sollten.

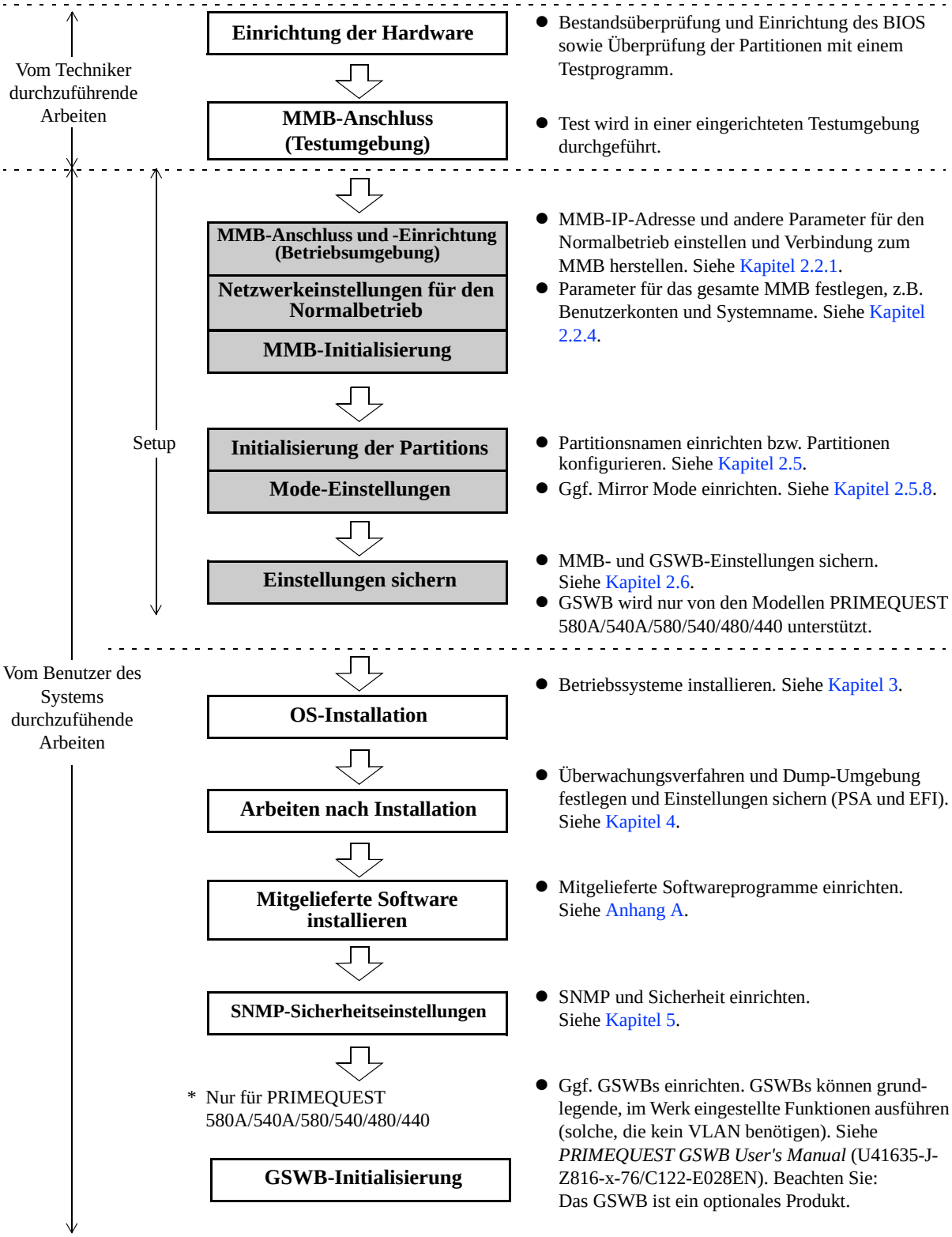

Vom Techniker durchzuführende Arbeiten
Einrichtung der Hardware
Bestandsüberprüfung und Einrichtung des BIOS sowie Überprüfung der Partitionen mit einem Testprogramm.
MMB-Anschluss (Testumgebung)
Test wird in einer eingerichteten Testumgebung durchgeführt.
Setup
MMB-Anschluss und -Einrichtung (Betriebsumgebung)
Netzwerkeinstellungen für den Normalbetrieb
MMB-Initialisierung
MMB-IP-Adresse und andere Parameter für den Normalbetrieb einstellen und Verbindung zum MMB herstellen. Siehe Kapitel 2.2.1.
Parameter für das gesamte MMB festlegen, z.B. Benutzerkonten und Systemname. Siehe Kapitel 2.2.4.
Initialisierung der Partitions
Mode-Einstellungen
Partitionsnamen einrichten bzw. Partitionen konfigurieren. Siehe Kapitel 2.5.
Ggf. Mirror Mode einrichten. Siehe Kapitel 2.5.8.
Einstellungen sichern
MMB- und GSWB-Einstellungen sichern. Siehe Kapitel 2.6.
GSWB wird nur von den Modellen PRIMEQUEST 580A/540A/580/540/480/440 unterstützt.
Vom Benutzer des Systems durchzuführende Arbeiten
OS-Installation
Betriebssysteme installieren. Siehe Kapitel 3.
Arbeiten nach Installation
Überwachungsverfahren und Dump-Umgebung festlegen und Einstellungen sichern (PSA und EFI). Siehe Kapitel 4.
Mitgelieferte Software installieren
Mitgelieferte Softwareprogramme einrichten. Siehe Anhang A.
SNMP-Sicherheitseinstellungen
SNMP und Sicherheit einrichten. Siehe Kapitel 5.
* Nur für PRIMEQUEST 580A/540A/580/540/480/440
GSWB-Initialisierung
Ggf. GSWBs einrichten. GSWBs können grundlegende, im Werk eingestellte Funktionen ausführen (solche, die kein VLAN benötigen). Siehe PRIMEQUEST GSWB User's Manual (U41635-J-Z816-x-76/C122-E028EN). Beachten Sie: Das GSWB ist ein optionales Produkt.

Abbildung 1.1 Installationsablauf

Anmerkung: Vor Beginn der Arbeiten, die der Benutzer des Systems ausführt, müssen qualifizierte Service-Techniker andere Arbeiten ausgeführt haben, einschließlich Inbetriebnahme des Systems, MMB-Setup, so weit sie hierfür zuständig sind, und Ausführen von Testprogrammen.

1.2.1 Für die Installation erforderliche Komponenten

Je nach Systemkonfiguration müssen Sie die folgenden Komponenten für die Installation bereithalten. Kontaktieren Sie den zuständigen Vertriebsmitarbeiter oder Kundendienst-Techniker, wenn Sie diese Dinge vorbereiten müssen.

Anm.: Wenn die PRIMEQUEST über ein LAN mit einem externen Switching Hub verbunden werden soll, wird ein externer Switching Hub benötigt.

- PC, der als Konsole benutzt werden kann
- LAN-Kabel (für das Benutzer-LAN)

KAPITEL 2 Installation

2.1 Installationsvorbereitung

Die Installation besteht grob aus den unten beschriebenen Schritten 1) bis 3). Bevor Sie mit der Installation beginnen, müssen Sie die IP-Adresse des Systems und einige andere Informationen ermittelt haben.

Wenn das System noch nicht eingeschaltet wurde, folgen Sie den in Anhang C, „Ein- und Ausschalten“ beschriebenen Anweisungen, um dies zu tun.

Hinweis: Management-LAN und Business-LAN müssen sich in unterschiedlichen Teilnetzen befinden.

(1) MMB einrichten (siehe Abschnitt 2.2)

Bevor Sie mit der Einrichtung des MMB beginnen können, benötigen Sie folgende Informationen:

- IP-Adresse, Hostname, Teilnetzmaske und Gateway-Adresse
- IP-Adresse des PCs, der als MMB-Konsole dienen soll
- Benutzerkonten
- Name der PRIMEQUEST (wird auch als SNMP-Systemname verwendet)
- Umgebung für das Management-VLAN

und anderes mehr.

(2) Partitionen einrichten (siehe Abschnitt 2.5)

Wenn Sie mehrere Partitionen konfigurieren wollen, müssen Sie vorab die Anzahl Partitionen und folgende Punkte festlegen:

- Partitionsnamen
- Partitionskonfiguration
- Home IOU
- Boot-Steuerung
- Systemspiegelung

und anderes mehr.

Anm.: Verwenden Sie den Namen des Hosts des in der Partition installierten Betriebssystems als Partitionsnamen, um die Partitionsverwaltung zu vereinfachen.

(3) GSWB einrichten (nur für PRIMEQUEST 580A/540A*/580/540/480/440) (siehe *PRIMEQUEST GSWB User's Manual* (U41635-J-Z816-x-76/C122-E028EN))

Grundlegende Funktionen von GSWB sind mit den Fabrikeinstellungen bereits möglich. Damit sind die Funktionen gemeint, die ein GSWB VLAN nicht verwenden. Im Handbuch *PRIMEQUEST GSWB User's Manual* (U41635-J-Z816-x-76/C122-E028EN) sind die für die Installation erforderlichen Einstellungen erläutert. Diese müssen nur durchgeführt werden, wenn Sie das GSWB benutzen wollen. Die folgenden Angaben sind erforderlich, um die Einstellungen durchführen zu können:

- Hostname, IP-Adresse des Hosts, Teilnetzmaske, Standard-Gateway
- Zu aktivierender Port

Hinweis: Diese Einstellungen sind für jedes GSWB erforderlich, das verwendet werden soll.

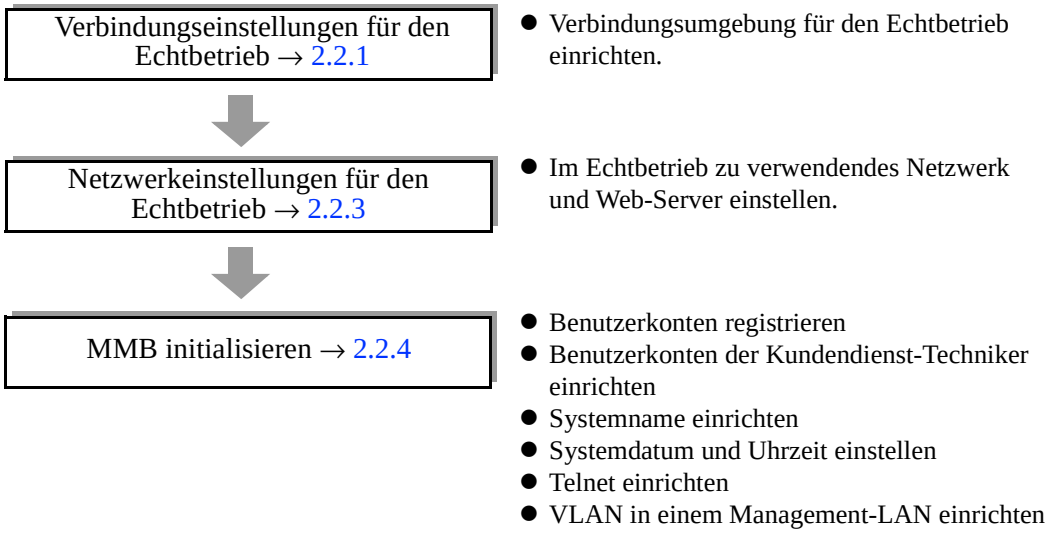
*: wird von Fujitsu Technology Solutions nicht unterstützt

2.2 MMB anschließen und einrichten

Wenn Sie mit der Einrichtung der MMBs beginnen, sind diese in einer von einem Kundendienst-Techniker erstellten Testumgebung eingebunden und Testprogramme sind durchgeführt worden. Für den tatsächlichen Betrieb müssen Sie die MMBs daher neu einstellen.

Legen Sie die IP-Adressen der MMBs fest und schließen Sie die relevanten Kabel an. Nachdem die MMBs angeschlossen sind, benutzen Sie das MMB Web-UI (Web User Interface), um Benutzerkonten einzurichten und Sicherheits-, Zeit- und sonstige MMB-Einstellungen vorzunehmen.

Die folgende Abbildung gibt einen Überblick über den Arbeitsablauf.


Verbindungseinstellungen für den Echtbetrieb → 2.2.1
Verbindungsumgebung für den Echtbetrieb einrichten.
Netzwerkeinstellungen für den Echtbetrieb → 2.2.3
Im Echtbetrieb zu verwendendes Netzwerk und Web-Server einstellen.
MMB initialisieren → 2.2.4
Benutzerkonten registrieren
Benutzerkonten der Kundendienst-Techniker einrichten
Systemname einrichten
Systemdatum und Uhrzeit einstellen
Telnet einrichten
VLAN in einem Management-LAN einrichten

2.2.1 Verbindung für den Echtbetrieb einstellen

Die für die Testumgebung gemachten Verbindungseinstellungen müssen für den Echtbetrieb geändert werden. Führen Sie folgende Schritte durch:

- IP-Adresse des als MMB-Konsole dienenden PCs festlegen (→ 2.2.1.1)
- MMB-Konsole an den MMB-Benutzerport anschließen (→ 2.2.1.2)
- Externe LAN-Verbindung der PRIMEQUEST (PRIMEQUEST 580A/540A*/580/540/480/440)
  (→ 2.2.1.3)

2.2.1.1 IP-Adresse des als MMB-Konsole dienenden PCs festlegen

Legen Sie auf dem PC, der als MMB-Konsole dienen soll, dessen IP-Adresse fest. Lesen Sie dazu das Handbuch des PCs.

2.2.1.2 MMB-Konsole an den MMB-Benutzerport anschließen

Schließen Sie die MMB-Konsole des Benutzers mit einem LAN-Kabel an den MMB-Benutzerport des Systems an. Die MMB-Konsole kann dann mit dem MMB-LAN kommunizieren.

In den PRIMEQUEST 580A/540A*/580/540/480/440-Systemen kommt eine redundante MMB-Konfiguration zum Einsatz, bei der ein MMB aktiv ist, während das andere sich im Standby-Modus befindet. Schließen Sie die MMB-Konsole an den aktiven Port an. Das ist in der Regel der MMB-Port 0 (ACT LED von MMB#0 leuchtet).

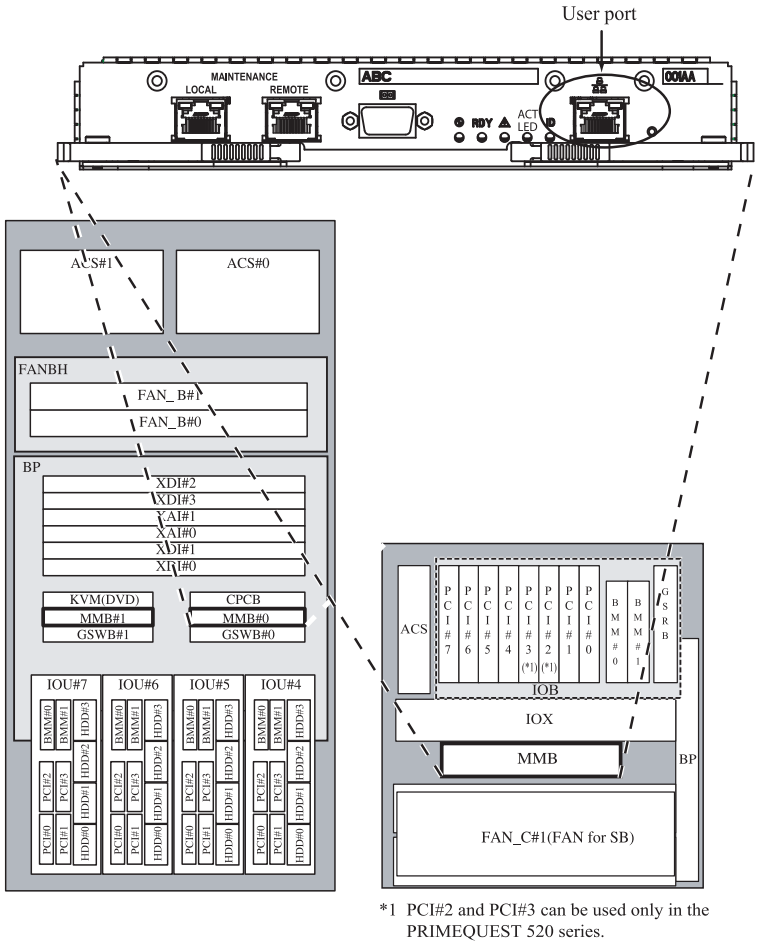


Abbildung 2.1 Position des MMB-Benutzerports

*: wird von Fujitsu Technology Solutions nicht unterstützt

Hinweis: BMM#1 wird nur in der PRIMEQUEST 500A*/500-Modellreihe unterstützt.

2.2.1.3 Externe LAN-Verbindung der PRIMEQUEST (PRIMEQUEST 580A/540A*/580/540/480/440)

Dieser Abschnitt beschreibt die Konfiguration der externen PRIMEQUEST LAN-Verbindungen und enthält einige diesbezügliche Hinweise. Es wird empfohlen, externe LAN-Verbindungen erst dann einzurichten, wenn alle Sicherheitseinstellungen vorgenommen worden sind.

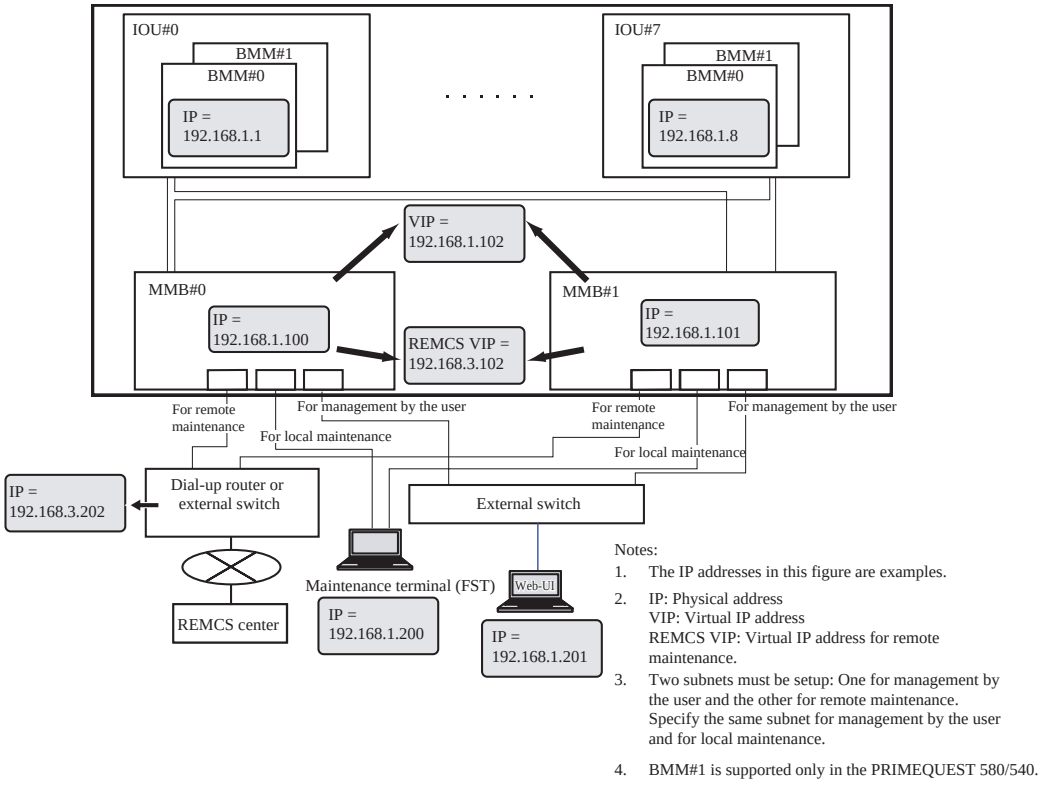


Abbildung 2.2 Management-LANs und IP-Adressen konfigurieren (PRIMEQUEST 580A/540A*/580/540/480/440)

Die Managementports 0 und 1 (MMB 0 und MMB 1) werden mit LAN-Kabeln an einen externen Switching Hub angeschlossen. Gleichzeitig wird dort ein PC für den MMB Web-UI-Betrieb angeschlossen.

Die physikalischen und virtuellen IP-Adressen von MMB 0 und MMB 1 müssen sich auf dasselbe Teilnetz beziehen.

*: wird von Fujitsu Technology Solutions nicht unterstützt

Jedes MMB verfügt über eine physikalische IP-Adresse (in der Abbildung oben 192.168.1.100 für MMB 0 und 192.168.1.101 für MMB 1) und eine virtuelle IP-Adresse (in der Abbildung oben 192.168.1.102). Die virtuelle IP-Adresse wird für die Kommunikation mit externen Zielen verwendet (Web-Browser, Wartungsterminal, REMCS*, usw.).

Hinweis:

- Wenn Sie ein Switching Hub benutzen wollen, der eine Loop-Guard-Funktion unterstützt (Spanning Tree-Protokoll oder Domain Separation), stellen Sie sicher, dass Sie diese Funktion unterdrücken. Entweder schalten Sie das Spanning Tree-Protokoll an dem Port aus, an dem der Hub an die Systemeinheit angeschlossen ist oder schalten Sie Domain Separation ein.
- Zur Kommunikation überträgt das MMB Pakete folgender Typen: NTP, Alarm-E-Mail, REMCS* und SNMP-Trap. Falls für das MMB sowohl eine physikalische IP-Adresse als auch eine virtuelle IP-Adresse eingestellt ist, wird die physikalische IP-Adresse als Absenderadresse verwendet.
  Unter den folgenden Bedingungen müssen Firewall, Mail und andere Dienste auf Durchlass der Pakete von MMB#0 und MMB#1 eingestellt werden:
  - Ziel ist ein externes System außerhalb der Firewall.
  - Die IP-Adressen werden vom verwendeten Mail-Server umgeleitet.

Falls darüber hinaus unter diesen Bedingungen der REMOTE MAINTENANCE-Port bei der PRIMEQUEST 580A/540A* verwendet wird, muss ebenfalls für die REMOTE MAINTENANCE-Pakete der Durchlass konfiguriert werden

Anm.:

- Die physikalischen IP-Adressen der MMBs werden in der Regel auch für Verbindungen mit PRIMECLUSTER benutzt.
- Gehen Sie wie im Folgenden beschrieben vor, wenn eine REMCS*-Verbindung eingerichtet werden soll. Nähere Einzelheiten finden Sie im Kapitel 6, „REMCS“ des Handbuchs *PRIMEQUEST 500/400 Series Reference Manual: Basic Operation/GUI/Commands* (U41633-J-Z816-x-76/C122-E003EN).

*: wird von Fujitsu Technology Solutions nicht unterstützt

- Internet-Verbindung:
  Die REMCS*-Ports werden vom externen Switch des Managementports aus über die Firewall mit dem externen Switching Hub oder mit dem REMCS*-Center verbunden.
- Punkt-zu-Punkt-Verbindung:
  Der REMCS*-Port jedes MMBs (MMB 0 und 1) wird über einen Wählrouter direkt mit dem REMCS*-Center verbunden.

2.2.1.4 Externe LAN-Verbindung der PRIMEQUEST (PRIMEQUEST 520A*/520/420)

Dieser Abschnitt beschreibt die Konfiguration der externen PRIMEQUEST LAN-Verbindungen und enthält einige diesbezügliche Hinweise. Es wird empfohlen, externe LAN-Verbindungen erst dann einzurichten, wenn alle Sicherheitseinstellungen vorgenommen worden sind.

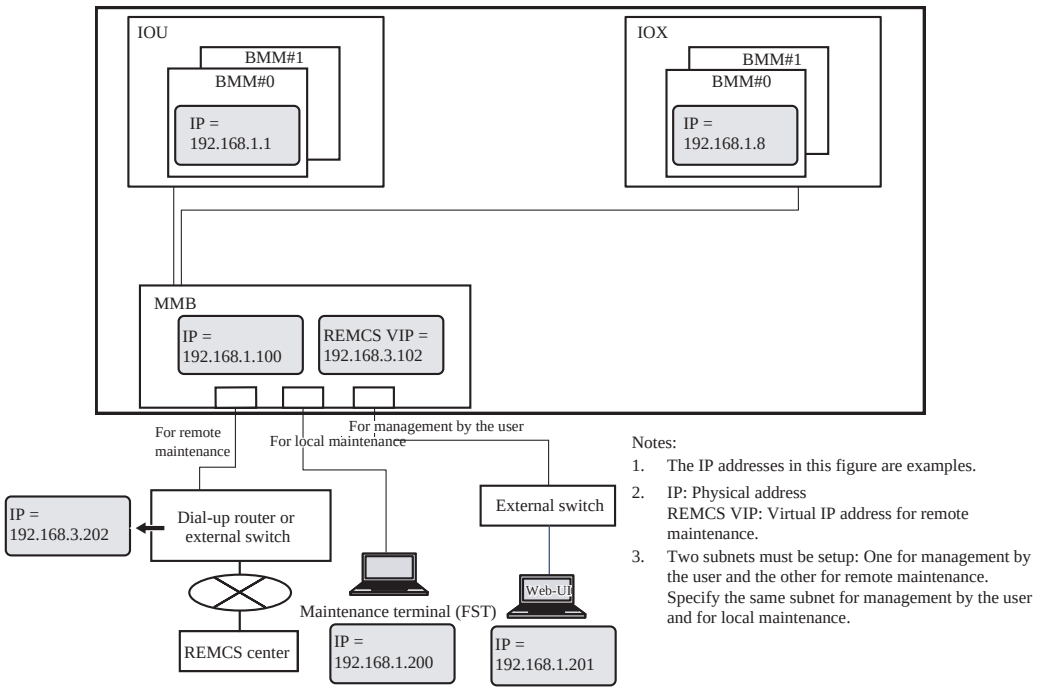


Abbildung 2.3 Management-LANs und IP-Adressen konfigurieren (PRIMEQUEST 520/420)

Das Managementport des MMB wird mit einem LAN-Kabel an einen externen Switching Hub angeschlossen. Gleichzeitig wird dort ein PC für den MMB Web-UI-Betrieb angeschlossen.

*: wird von Fujitsu Technology Solutions nicht unterstützt

Das MMB verfügt über eine physikalische IP-Adresse (in der Abbildung oben 192.168.1.100). Die IP-Adresse wird für die Kommunikation mit externen Zielen verwendet (Web-Browser, Wartungsterminal, REMCS*, usw.).

Hinweis:

- Wenn Sie ein Switching Hub benutzen wollen, der die Funktion zur Schleifenvermeidung unterstützt (Spanning Tree-Protokoll oder Domain Separation), stellen Sie sicher, dass Sie diese Funktion unterdrücken. Entweder schalten Sie das Spanning Tree-Protokoll an dem Port aus, an dem der Hub an die Systemeinheit angeschlossen ist oder schalten Sie Domain Separation ein.
- Zur Kommunikation überträgt das MMB Pakete folgender Typen: NTP, Alarm-E-Mail, REMCS* und SNMP-Trap. Falls für das MMB sowohl eine physikalische IP-Adresse als auch eine virtuelle IP-Adresse eingestellt ist, wird die physikalische IP-Adresse als Absenderadresse verwendet.
  Unter den folgenden Bedingungen müssen Firewall, Mail und andere Dienste auf Durchlass der Pakete von MMB#0 und MMB#1 eingestellt werden:
  - Ziel ist ein externes System außerhalb der Firewall.
  - Die IP-Adressen werden vom verwendeten Mail-Server umgeleitet.

Falls darüber hinaus unter diesen Bedingungen der REMOTE MAINTENANCE-Port bei der PRIMEQUEST 520A* verwendet wird, muss ebenfalls für die REMOTE MAINTENANCE-Pakete der Durchlass konfiguriert werden

Anm.:

- Die IP-Adressen des MMBs werden in der Regel auch für Verbindungen mit PRIMECLUSTER benutzt.
- Gehen Sie wie im Folgenden beschrieben vor, wenn eine REMCS*-Verbindung eingerichtet werden soll. Nähere Einzelheiten finden Sie im Kapitel 6 „REMCS“ des Handbuchs *PRIMEQUEST 500/400 Series Reference Manual: Basic Operation/GUI/Commands* (U41633-J-Z816-x-76/C122-E003EN).

*: wird von Fujitsu Technology Solutions nicht unterstützt

- Internet-Verbindung:
  Die REMCS*-Ports werden vom externen Switch des Management-ports aus über die Firewall mit dem externen Switching Hub oder mit dem REMCS-Center verbunden.
- Punkt-zu-Punkt-Verbindung:
  Der REMCS*-Port jedes MMBs (MMB 0 und 1) wird über einen Wählrouter direkt mit dem REMCS*-Center verbunden.

2.2.2 An- und Abmelden beim MMB und Fensterkonfiguration

Die in Abschnitt 2.2.3, „Netzwerkeinstellungen für den Echtbetrieb“, 2.2.4, „MMB initialisieren“ und 2.5, „Partition initialisieren“ beschriebenen Operationen werden über das MMB Web-UI ausgeführt. In diesem Abschnitt wird erläutert, wie Sie sich beim MMB Web-UI anmelden und was die Anzeigen bedeuten.

- An- und Abmelden bei der MMB Web-UI (→ 2.2.2.1)
- Elemente des Web-UI-Fensters (→ 2.2.2.2)

*: wird von Fujitsu Technology Solutions nicht unterstützt

2.2.2.1 An- und Abmelden bei der MMB Web-UI

Im Folgenden wird beschrieben, wie Sie sich beim MMB Web-UI anmelden.

Um sich beim MMB Web-UI anzumelden, müssen Sie entweder die virtuelle oder die physikalische IP-Adresse des aktiven MMBs oder den der IP-Adresse entsprechenden vollständigen Domänennamen (FQDN - Fully Qualified Domain Name) angeben.

Der DNS-Server muss bereits festgelegt worden sein, damit der FQDN benutzt werden kann.

⚠ ACHTUNG

Fehlfunktion

Das MMB Web-UI (Web User Interface) unterstützt die folgenden Browser. Andere Browser zeigen die Web-UI möglicherweise nicht korrekt an.

- Microsoft® Internet Explorer Version 5.5 (SP2) oder höher
- Netscape Version 7.02 oder höher

Anmelden

1 Starten Sie den Web-Browser.

Anm. 1: Die Verwendung von JavaScript muss vom MMB Web-UI durch die entsprechenden Browser-Einstellungen zugelassen sein.

Anm. 2: Das Herunterladen von Daten über das MMB Web-UI muss durch die entsprechenden Browser-Einstellungen zugelassen sein.

2 Geben Sie die folgende URL ein.

Standard	http://knotenname:adminport
SSL	https://knotenname:adminport

knotenname: der FQDN oder die IP-Adresse des MMB.

adminport: die Portnummer des MMB-Managementports (Default-Wert: 8081 für Standard bzw. 432 für SSL).

3 Geben Sie den Namen und das Kennwort eines Benutzerkontos ein und klicken Sie dann auf die Schaltfläche [Login].

Anm: Wenn der Browser zum ersten Mal gestartet wird oder wenn eine Einstellungsänderung nicht durchgeführt wird, gelten das Standardbenutzerkonto und -kennwort. Sie werden anschließend aufgefordert, ein neues Kennwort einzugeben.

Benutzername	Administrator
Kennwort	Vom Kundendienst-Techniker bei der Installation vergebenes Kennwort.

Abmelden

1 Klicken Sie auf die Schaltfläche [Logout] oben rechts im Browser-Fenster, um das MMB Web-UI wieder zu verlassen.

Anm.: Auf andere Funktionen können Sie über die Menüs und Untermenüs zugreifen.

2.2.2.2 Elemente des Web-UI-Fensters

In diesem Abschnitt werden die Informationen beschrieben, die im Web-UI-Fenster (Beispiel PRIMEQUEST 580A/540A/580/540/480/440) angezeigt werden können.

Aufbau des Web-UI-Fensters

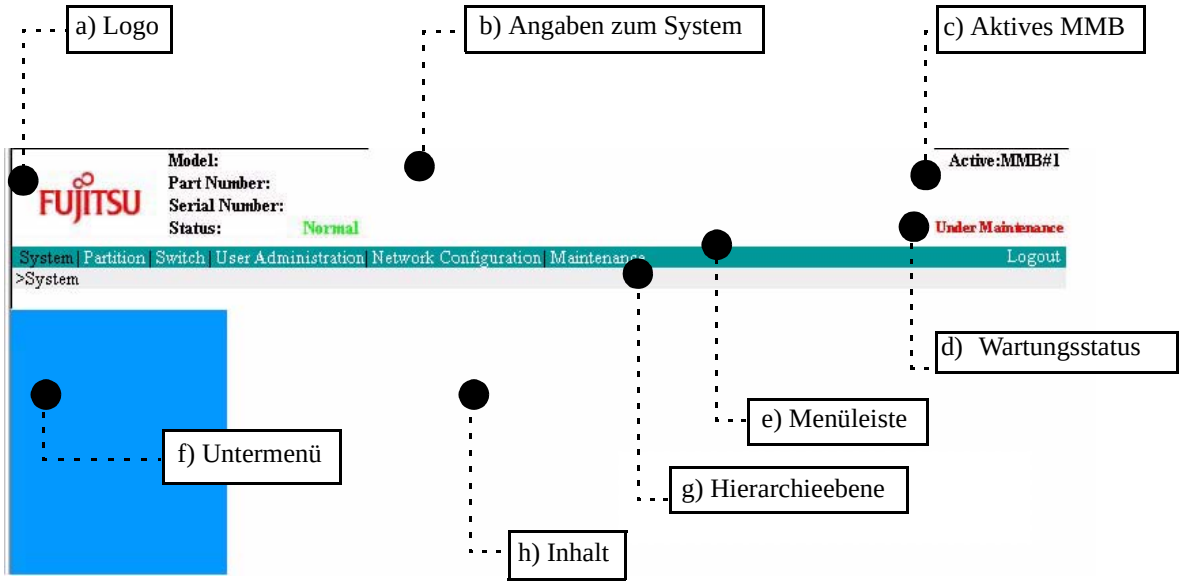


Abbildung 2.4 Aufbau des Fensters [Web-UI Frame Information]

a) Logo

Klicken Sie auf das Fujitsu Logo, um auf die Fujitsu Technology Solutions Homepage zu gelangen.

b) Angaben zum System

In diesem Bereich werden die folgenden Informationen angezeigt:

- [Model]
  Bezeichnung des PRIMEQUEST Modells
  (Product Info Product Name of operation panel FRU)
- [Part Number]
  Die PRIMEQUEST Teilenummer
  (Product Info Product Part/Model Number of operation panel FRU)

  Anm.: Nehmen Sie Kontakt zu einem Kundendienst-Techniker auf, wenn „Read Error“ angezeigt wird.
- [Serial Number]
  Die Seriennummer der PRIMEQUEST

  Anm.: Nehmen Sie Kontakt zu einem Kundendienst-Techniker auf, wenn „Read Error“ angezeigt wird.
- [Status]
  Status der gesamten PRIMEQUEST. Es gibt die drei folgenden Zustandsmeldungen. Durch Anklicken können Sie das Fenster [System Event Log] mit den Systemereignissen öffnen.

Tabelle 2.1 Systemstatus-Anzeige

Status	Farbe	Symbol
Normal	Grün	Keines
Warning	Gelb	Schwarzes „!“ in gelbem Dreieck
Error	Rot	Weißes „x“ in rotem Kreis

c) Aktives MMB

Die Nummer des MMBs, mit dem das MMB Web-UI verbunden ist.

d) Wartungsstatus

Wenn ein Kundendienst-Techniker Wartungsarbeiten an dem Gerät durchführt, erschein in diesem Bereich in Orange die Anzeige „Under Maintenance“. Werden keine Wartungsarbeiten durchgeführt, erscheint hier keine Angezeige.

e) Menüleiste

Hier wird die oberste Menüebene angezeigt. Wenn Sie den Mauszeiger auf ein Menü positionieren, um dieses auszuwählen, erscheint es schwarz, ein nicht ausgewähltes Menü erscheint weiß.

- [System], [Partition], [Switch], [User Administration], [Network Configuration], [Maintenance]
  Klicken Sie auf eines der Menüs, um die Menüeinträge zu betrachten (siehe Abschnitt g).

  Hinweis: [Switch] steht nur bei den Modellen PRIMEQUEST 520A/520/420 zur Verfügung sowie bei den Modellen PRIMEQUEST 580A/540A*/580/540/480/440 mit eingebautem GTHB.

- [Logout]
  Klicken Sie hier, um das MMB Web-UI zu verlassen.

f) Hierarchieebene

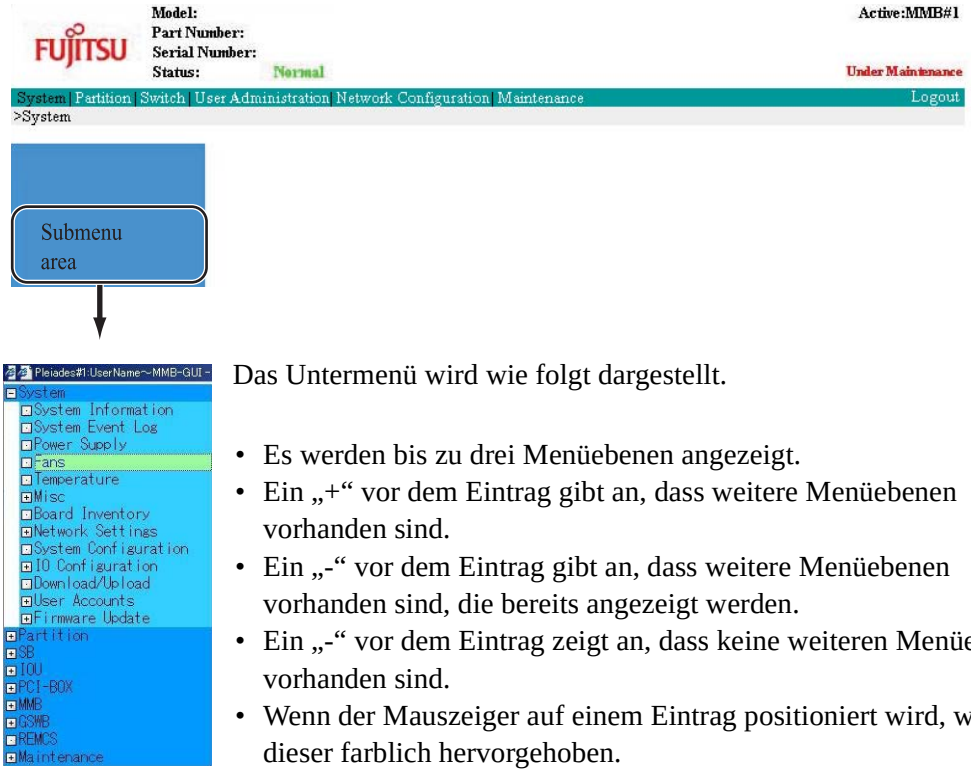
Hierarchie
Die Hierarchieebenen, die der Benutzer auf dem Weg von der obersten Menüebene zum aktuell angezeigten Untermenü durchläuft, werden hier angezeigt. Klicken Sie auf das hier angezeigte Menü, um den Inhalt des Menüfensters zu betrachten.

Beispiel: >System>System Status

g) Untermenü

Es wird das Untermenü des in der Navigationsleiste ausgewählten Menüs angezeigt.

*: wird von Fujitsu Technology Solutions nicht unterstützt



Das Untermenü wird wie folgt dargestellt.

- Es werden bis zu drei Menüebenen angezeigt.
- Ein „+“ vor dem Eintrag gibt an, dass weitere Menüebenen vorhanden sind.
- Ein „-“ vor dem Eintrag gibt an, dass weitere Menüebenen vorhanden sind, die bereits angezeigt werden.
- Ein „-“ vor dem Eintrag zeigt an, dass keine weiteren Menüebenen vorhanden sind.
- Wenn der Mauszeiger auf einem Eintrag positioniert wird, wird dieser farblich hervorgehoben.
- Die Hintergrundfarbe des Eintrags ändert sich.

Abbildung 2.5 Untermenü

h) Inhalt

In diesem rechten Teilfenster wird das Fenster des Untermenüs angezeigt.

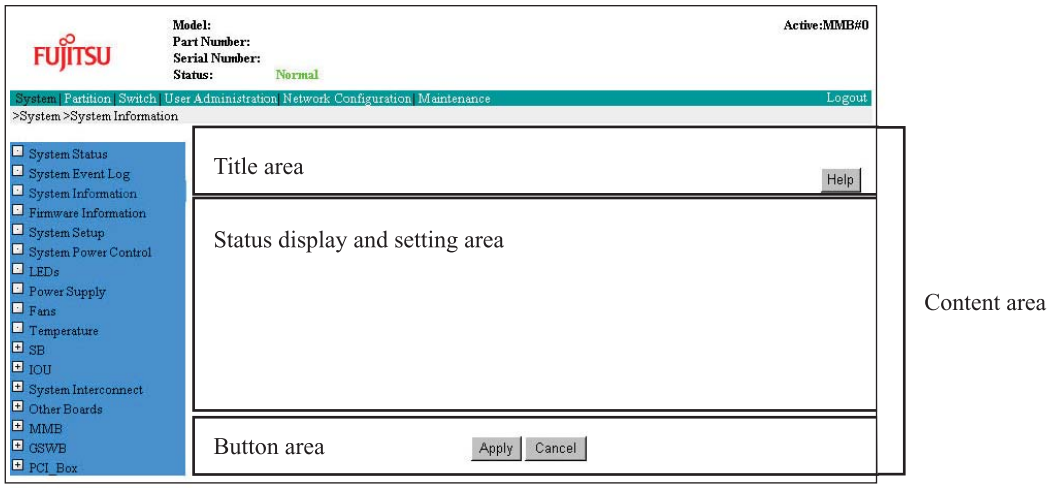


Abbildung 2.6 Aufbau des rechten Teilfensters

Das rechte Teilfenster ist in drei Bereiche untergliedert.

- Überschrift

  Hier wird die Überschrift des Inhaltsbereichs angezeigt.

  - In diesem Bereich befindet sich auch eine Schaltfläche [Help], über die Sie auf die Systemhilfe zugreifen können sowie eine Schaltfläche [Refresh], mit der Sie die Anzeige aktualisieren können.
  - Die Schaltfläche [Refresh] bezieht sich nur auf den Inhalt des Fensters.
  - Die Schaltfläche [Refresh] steht nicht in allen Fenstern zur Verfügung. Wenn in einem Fenster nur Einstellungen vorgenommen werden können, wird sie nicht angeboten.

    Anm.: Sie können die Aktualisierungsrate im Menü [Network Configuration] mit der Funktion [Refresh Rate] festlegen.

  - Fenster mit der Schaltfläche [Refresh] werden automatisch aktualisiert (Ausnahme PSA).
  - Dieser Bereich wird nicht mit den Bereich [Status und Einstellungen] geblättert.

- Status und Einstellungen

In diesem Bereich des Fensters werden Status und Einstellungen angezeigt. Statusanzeigen für „Normal“, „Warning“ und „Error“ werden jeweils mit einer anderen Hintergrundfarbe dargestellt.

Tabelle 2.2 Status anzeige

Status	Hintergrundfarbe
Normal	Normaler Hintergrund des Fensters.
Warning	Farbe für Warnungen (gelb)
Error	Farbe für Fehler (rot)

Wenn der Benutzer nur über Leseberechtigung verfügt, sind alle Eingabefelder, Auswahlfelder und Kontrollkästchen ausgegraut (deaktiviert).

- Schaltflächen

  In diesem Bereich stehen Schaltflächen zur Verfügung, mit denen die Inhalte des Bereichs [Status und Einstellungen] übernommen oder verworfen werden können. In der Regel werden die Schaltflächen [Apply] und [Cancel] angeboten.
  Wenn in einem Fenster nur Daten angezeigt werden und keine Benutzereingaben erforderlich sind, wird dieser Teilbereich nicht dargestellt.

Vorgehensweise

Die grundlegende Vorgehensweise ist wie folgt:

1 Wählen Sie in der Menüleiste ein Menü aus.
Das entsprechende Untermenü wird angezeigt.

2 Wählen Sie aus dem Untermenü einen Eintrag aus.
Das Fenster des gewählten Eintrags wird im rechten Teilfenster angezeigt.

3 Überprüfen Sie die Angaben und nehmen Sie gegebenenfalls erforderliche Änderungen vor.
Klicken Sie auf die Schaltfläche [Apply], um die Einstellungen zu übernehmen.
Klicken Sie auf die Schaltfläche [Cancel], um die Änderungen rückgängig zu machen.

Anm.: Klicken Sie auf die Schaltfläche [←] (Zurück) in der Symbolleiste des rechten Teilfensters, um zur vorherigen Hierarchieebene zurückzukehren.
Das Fenster der vorherigen Hierarchieebene wird im rechten Teilfenster angezeigt.

Hinweis: Wird das MMB WEB-UI vom Internet Explorer aus benutzt und wird die Dialogbox zur Bestätigung von Prozessausführungen oder der Mitteilung über das Prozessende länger als zwei Minuten ausgegeben, wird die Verbindung zum MMB WEB-UI unterbrochen. Melden Sie sich in diesem Fall neu beim MMB WEB-UI an.

Notationskonventionen

Die in diesem Handbuch beschriebenen Aktionen werden in folgendem Format dargestellt:

- Auswahl eines Menüeintrags in der Web-UI
  [ ] → [ ]
  Beispiel: Anzeige des Fensters [System Status]
  Klicken Sie auf [System] → [System Status]. (Einträge in der angegebenen Reihenfolge auswählen.)
- Mehrere Menüs derselben Hierarchieebene werden wie folgt dargestellt:
  [ ]/[ ]/[ ]/[ ]
  Beispiel: Anzeige des Fensters [Port Configuration] für die IO Unit, den Front Panel, den Port Channel oder die Partition
  Klicken Sie auf [Switch] → [GSWB#x] → [Port] → [Port Configuration] → [IOU]/[Front Panel]/[port-channel]/[Partition].

- Eine aus mehreren möglichen Komponenten (das betreffende Web-UI wird durch eine Zahl angegeben.)
  Komponentenname#x
  Beispiel Partition in der zweiten Hierarchieebene
  Klicken Sie auf [Partition] → [Partition#x] → [Mode].

Tritt einer der MMB Fehler- oder Warnzustände aus der folgenden Liste „Überprüfungsbedingungen bei Betriebsstörung“ auf, brechen Sie die aktuelle Aktion ab. Wenden Sie sich an Ihren Kundendienst-Techniker.

- Überprüfungsbedingungen bei Betriebsstörung
  - Die Alarm-LED auf dem MMB leuchtet.
  - Die Active LEDs auf MMB#0 und MMB#1 leuchten nicht.
  - Es kann keine Verbindung zum MMB Web-UI aufgebaut werden.
  - Die Alarm-LEDs auf mehr als zwei Boards der Systemeinheit leuchten.
  - Auf dem MMB Web-UI wird „ReadError“ ausgegeben.
  - Im Fenster [System Status] des MMB Web-UI wird für den Zustand jeder Einheit „Not Present“ ausgegeben.

2.2.3 Netzwerkeinstellungen für den Echtbetrieb

Dieser Abschnitt beschreibt die für den tatsächlichen Betrieb erforderlichen Einstellungen. Führen Sie diese für den von Ihnen verwendeten Betriebsmodus durch.

- MMB-Netzwerk einrichten (PRIMEQUEST 580A/540A*/580/540/480/440) (→ 2.2.3.1)
- MMB-Netzwerk einrichten (PRIMEQUEST 520A/520/420) (→ 2.2.3.2)
- Telnet-Parameter einstellen (→ 2.2.3.3)
- DNS-Server einrichten (→ 2.2.3.4)

Abschnitt 2.6, „Konfiguration sichern“, beschreibt, wie Sie die gemachten Einstellungen sichern.

Anm.: Hierzu sind Systemverwalterrechte erforderlich.

2.2.3.1 MMB-Netzwerk einrichten (PRIMEQUEST 580A/540A*/580/540/480/440)

Geben Sie die virtuelle IP-Adresse an, über die auf die Web-UI zugegriffen wird sowie die physikalische IP-Adresse, die der MMB-Schnittstelle zugewiesen ist.

Diese Angaben sind möglicherweise bereits vom Kundendienst-Techniker gemacht worden. Fahren Sie mit dem nächsten Schritt fort, wenn diese Angaben nicht geändert werden müssen.

Hinweise:

- Spezifizieren Sie dasselbe Subnet für die physikalische und virtuelle IP-Adresse des MM MMB#0 und MMB#1.
- Wenn eine virtuelle IP-Adresse eingestellt ist und auf das PRIMEQUEST-System von einem anderen System oder Gerät zugegriffen wird (z. B. von einem Web-Browser aus, einem Wartungs-Terminal, dem REMCS* etc.), dann wird über die virtuelle IP-Adresse zugegriffen. Deshalb ist es nicht möglich, auf das MMB-Web-UI unter Angabe der physikalischen IP-Adresse des MMB #0 oder MMB #1 zuzugreifen.

Anm.:

*: wird von Fujitsu Technology Solutions nicht unterstützt

- Wenn Sie die Angaben für [MMB#0 IP Address] oder [MMB#1 IP Address] ändern und dann [Apply] anklicken, wird das Netzwerk kurzfristig gestoppt und das Web-UI geschlossen, damit die Änderungen übernommen werden können. Sie können das Web-UI über den entsprechenden Menüeintrag wieder öffnen.
- Wenn die IP-Adresse geändert wird, wird die Verbindung zur MMB Web-UI unterbrochen. Melden Sie sich beim MMB Web-UI neu an.

Vorgehensweise

1 Wählen Sie [Network Configuration] → [Network Interface].
Das Fenster [Network Interface] wird angezeigt.

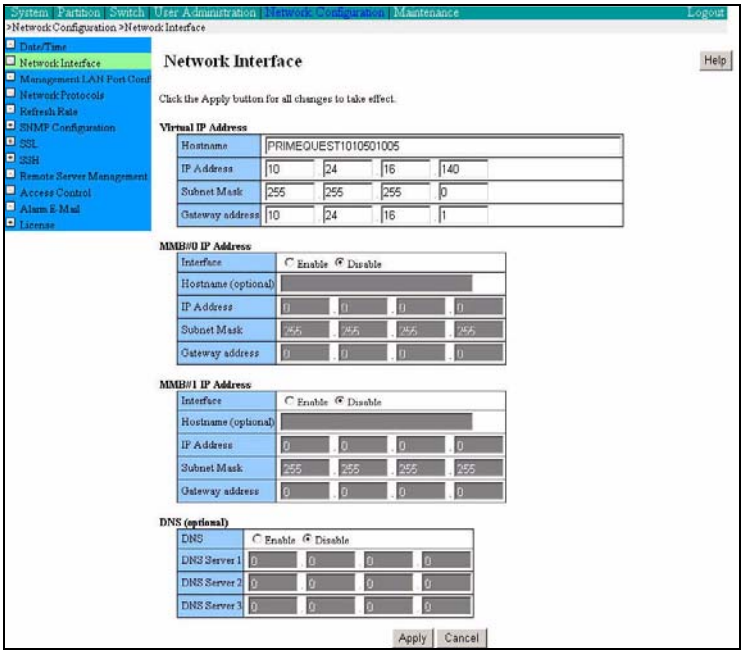


Abbildung 2.7 Fenster [Network Interface]
(PRIMEQUEST 580A/540A/580/540/480/440)

2 Geben Sie unter [Virtual IP Address] die IP-Adresse, Teilnetzmaske und Gateway-Adresse an. Der Hostname muss angegeben werden.

Tabelle 2.3 Feldnamen und mögliche Eingaben im Fenster [Network Interface]

Feldname	Beschreibung
Hostname	Name des Rechners eingeben.
IP Address	Virtuelle IP-Adresse für den Zugriff auf das Web-UI eingeben.
Subnet Mask	Teilnetzmaske eingeben.
Gateway Address	IP-Adresse des Gateways eingeben.

3 Aktivieren Sie im Feld [Interface] unter [MMB#0 IP Address] bzw. [MMB#1 IP Address] das Optionsfeld [Enable] und geben Sie die Werte ein.
Geben Sie die zuzuweisende physikalische IP-Adresse an.

Tabelle 2.4 Feldnamen und mögliche Eingaben im Fenster [Network Interface]

Feldname	Beschreibung
Hostname	Name des Rechners eingeben.
IP Address	IP-Adresse eingeben.
Subnet Mask	Teilnetzmaske eingeben.
Gateway Address	IP-Adresse des Gateways eingeben.

4 Klicken Sie auf [Apply], um alle angegebenen Einstellungen zu übernehmen.
Hinweis: Wenn eine falsche IP-Adresse angebeben wird oder eine der anderen Angaben falsch ist, wird das MMB Web-UI nicht angezeigt. Schließen Sie in diesem Fall ggf. einen PC an den COM-Port des MMB an und stellen Sie dort die richtigen Werte ein.
Einzelheiten über die Einstellung der Parameter finden Sie in Anhang B, „Installation“.

2.2.3.2 MMB-Netzwerk einrichten (PRIMEQUEST 520A*/520/420)

Geben Sie die IP-Adresse an, über die auf die Web-UI zugegriffen wird.

Diese Angaben sind möglicherweise bereits vom Kundendienst-Techniker gemacht worden. Fahren Sie mit dem nächsten Schritt fort, wenn diese Angaben nicht geändert werden müssen.

Anm.: Wenn die IP-Adresse geändert wird, wird die Verbindung zur MMB Web-UI unterbrochen. Melden Sie beim MMB Web-UI neu an.

Vorgehensweise

1 Wählen Sie [Network Configuration] → [Network Interface].
Das Fenster [Network Interface] wird angezeigt.

*: wird von Fujitsu Technology Solutions nicht unterstützt

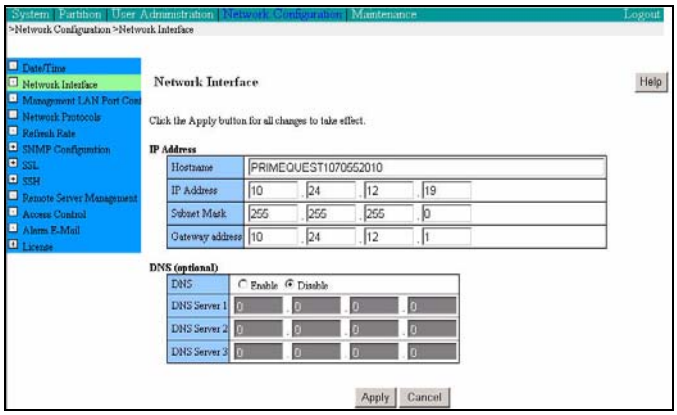


Abbildung 2.8 Das Fenster [Network Interface] (PRIMEQUEST 520A*/520/420)

2 Geben Sie unter [IP Address] die IP-Adresse, Teilnetzmaske und Gateway-Adresse an. Der Hostname muss angegeben werden.

Tabelle 2.5 Feldnamen und mögliche Eingaben im Fenster [Network Interface]

Feldname	Beschreibung
Hostname	Name des Rechners eingeben.
IP Address	IP-Adresse für den Zugriff auf das Web-UI eingeben.
Subnet Mask	Teilnetzmaske eingeben.
Gateway Address	IP-Adresse des Gateways eingeben.

3 Klicken Sie auf [Apply], um die Einstellungen zu übernehmen.

Hinweis:Wenn eine falsche IP-Adresse angebeben wird oder einer der anderen Angaben falsch ist, wird das MMB Web-UI nicht angezeigt. Schließen Sie in diesem Fall ggf. einen PC an den COM-Port des MMB an und stellen Sie dort die richtigen Werte ein.

Einzelheiten über die Einstellung der Parameter finden Sie in Anhang B, „Installation“.

*: wird von Fujitsu Technology Solutions nicht unterstützt

2.2.3.3 Telnet-Parameter einstellen

Geben Sie die Telnet-Parameter für das MMB ein. Hierzu sind Systemverwalter-berechtigungen erforderlich.

Vorgehensweise

1 Wählen Sie [Network Configuration] → [Network Protocols].
Das Fenster [Network Protocols] wird angezeigt.

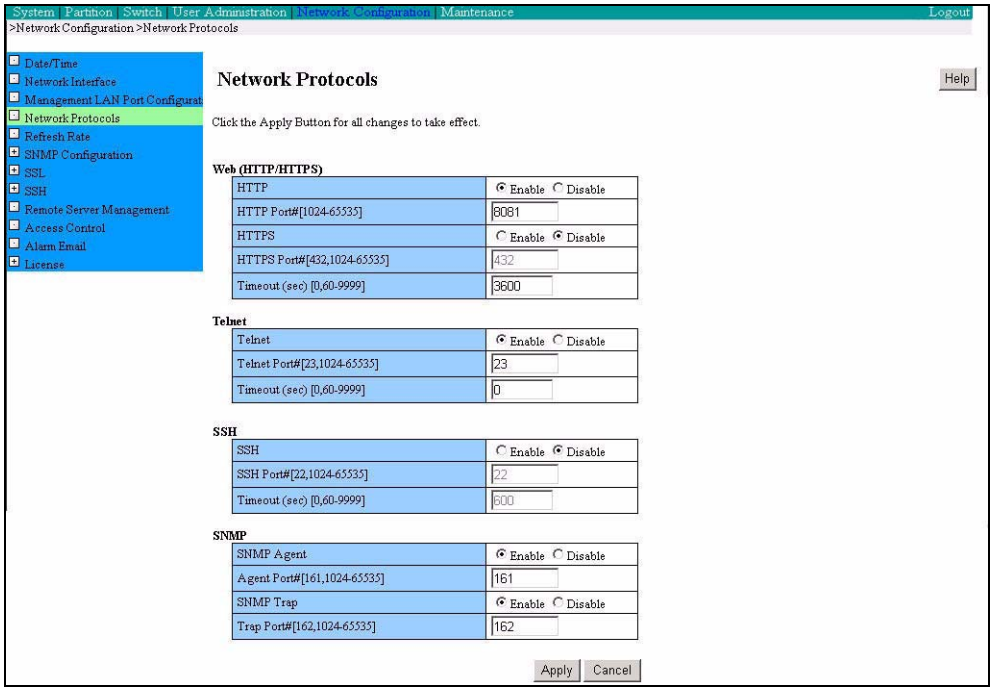


Abbildung 2.9 Das Fenster [Network Protocols]

2 Machen Sie unter [Telnet] die im Folgenden beschriebenen Einstellungen.

Tabelle 2.6 Feldnamen und mögliche Eingaben im Fenster [Network Interface]

Feldname	Beschreibung
<Telnet>	
Telnet	Telnet aktivieren bzw. deaktivieren Voreinstellung: [Disable]
Telnet Port	Für Telnet zu verwendender Port Voreinstellung: 23
Timeout	Legt dem Zeitraum fest, in dem über Telnet Daten empfangen werden müssen, bevor die Verbindung abgebrochen wird. Voreinstellung: 600 Sekunden

3 Klicken Sie auf [Apply].

2.2.3.4 DNS-Server einrichten

Geben Sie den DNS-Server an, damit dieser benutzt werden kann. Dies kann auch zu einem späteren Zeitpunkt geschehen.

Vorgehensweise

1 Wählen Sie auf [Network Configuration] → [Network Interface].
Das Fenster [Network Interface] wird angezeigt.

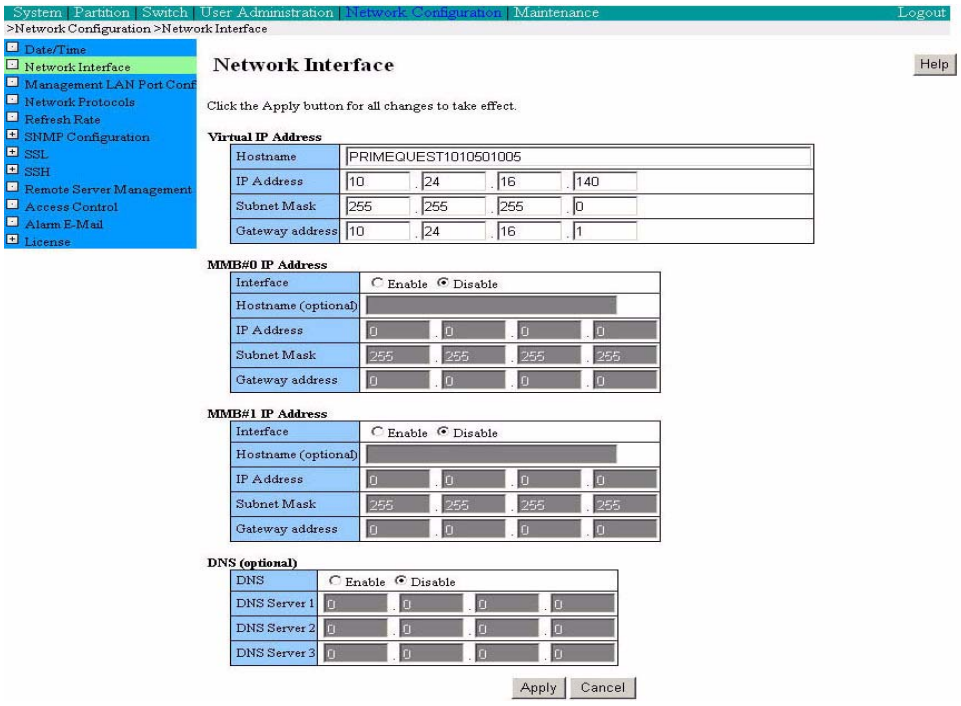


Abbildung 2.10 Fenster [Network Interface]
(PRIMEQUEST 580A/540A*/580/540/480/440)

*: wird von Fujitsu Technology Solutions nicht unterstützt

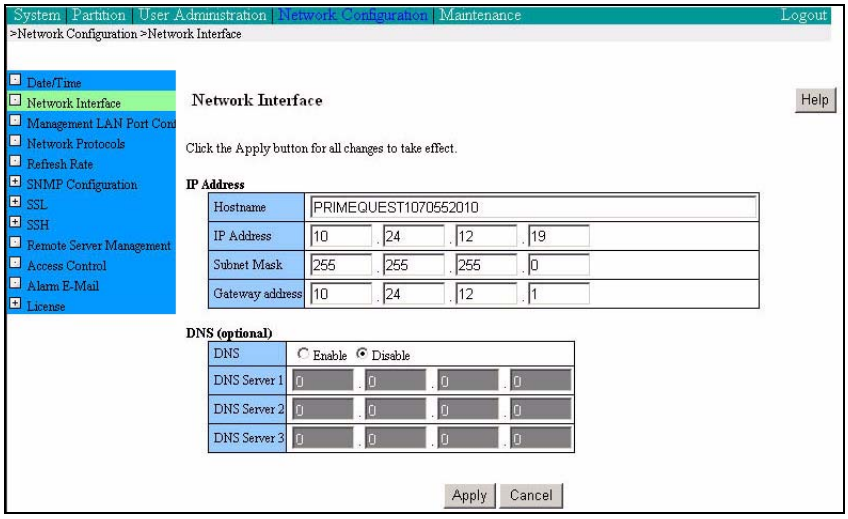


Abbildung 2.11 Das Fenster [Network Interface] (PRIMEQUEST 520A*/520/420)

2 Aktivieren Sie im Feld [DNS] unter [DNS (optional)] das Optionsfeld [Enable] und geben Sie die Werte ein.

Tabelle 2.7 Feldnamen und mögliche Eingaben im Fenster [Network Interface]

Feldname	Beschreibung
DNS	Geben Sie an, ob der DNS-Server benutzt werden soll. Enabled: DNS-Server benutzen. Disabled: DNS-Server nicht benutzen. Standardeinstellung [Disabled].
DNS Server1	IP-Adresse des ersten DNS-Servers angeben.
DNS Server2	IP-Adresse des zweiten DNS-Servers angeben.
DNS Server3	IP-Adresse des dritten DNS-Servers angeben.

3 Wenn Sie alle Angaben gemacht haben, klicken Sie auf [Apply].

2.2.3.5 SMTP-Einstellungen

Richten Sie das MMB SMTP (Simple Mail Transfer Protocol) ein, d.h. legen Sie fest, ob Fehler während des laufenden Betriebs per E-Mail gemeldet werden sollen. Wenn Sie Fehler per E-Mail gemeldet bekommen wollen, müssen Sie auch die Fehlerkategorie und die Zieladresse für E-Mails festlegen.

*: wird von Fujitsu Technology Solutions nicht unterstützt

Fehler per E-Mail melden

- Vorgehensweise

1 Wählen Sie [Network Configuration] → [Alarm E-Mail].
Das Fenster [Alarm E-Mail] wird angezeigt.

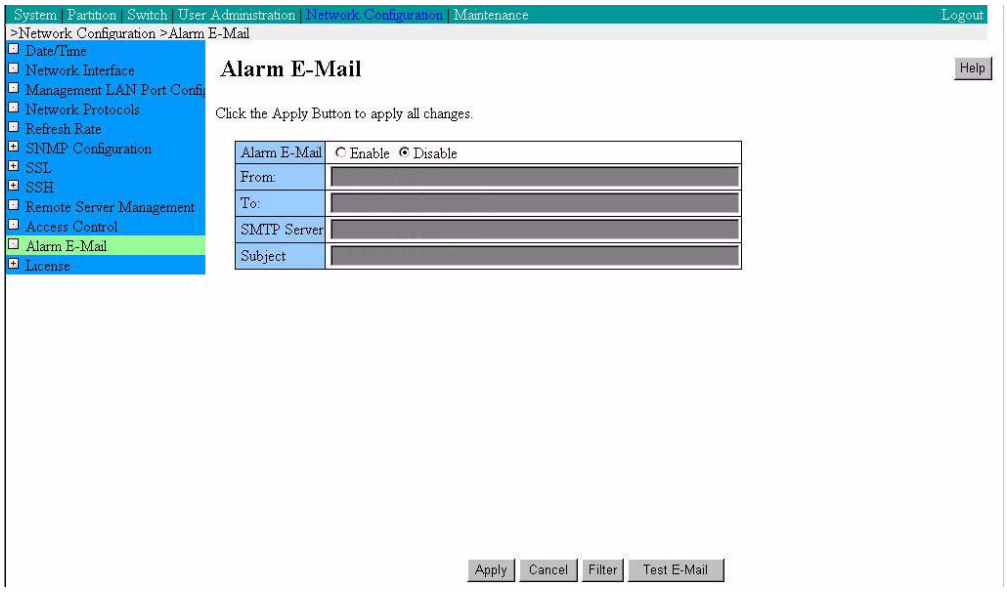


Abbildung 2.12 Das Fenster [Alarm E-Mail]

2 Geben Sie die erforderlichen Daten ein.

Tabelle 2.8 Feldnamen und mögliche Eingaben im Fenster [Alarm E-Mail]

Feldname	Beschreibung
Alarm E-Mail	Legt fest, ob ein Fehler per E-Mail gemeldet werden soll. Aktivieren Sie [Enable].
From:	E-Mailadresse des Senders.
To:	E-Mailadresse des Empfängers.
SMTP Server	IP-Adresse oder FQDN des SMTP-Servers. Ein FQDN kann nur angegeben werden, wenn ein DNS-Server eingerichtet wurde.
Subject	Inhalt der Betreffzeile der E-Mail.

3 Klicken Sie auf die relevante Schaltfläche.
- Um die Einstellungen durchzuführen, klicken Sie auf [Filter].
- Um die Einstellungen zu übernehmen, klicken Sie auf [Apply].
- Um eine Test-E-Mail zu senden, klicken Sie auf [Test E-Mail].

[Beginn der Korrektur gemäß Handbuch-Errata 2008/12/18]

~~Hinweis:~~ ~~Bevor Sie einen FQDN angeben können, muss ein DNS-Server eingerichtet worden sein. Wählen Sie dazu [Network Configuration] → [Network Interface].~~

Hinweis:
- Für den Alarm-E-Mail-Versand zum SMTP-Server hängt die Absenderadresse vom Format ab, das in [Network Configuration] → [Network Interface] eingestellt ist:

FQDN-Format	root@[Hostname]
Nicht-FQDN-Format	root@[Hostname].[Hostname]

  Die Mail-Adresse, die im From-Feld eingestellt ist, wird als Absenderadresse für das Versenden zur (To) Empfängeradresse verwendet.
- Der DNS-Server muss bereits eingestellt sein, um den FQDN für den SMTP-Servernamen einzustellen. Der DNS-Server kann durch Anwahl von [Network Configuration] → [Network Interface] eingestellt werden.

[Ende der Korrektur gemäß Handbuch-Errata 2008/12/18]

Einstellungen für die Übertragung von E-Mails

- Gehen Sie wie folgt vor:

1 Klicken Sie im Fenster [Alarm E-mail] auf die Schaltfläche [Filter]
Das Fenster [Alarm E-Mail Filtering Condition] erscheint.

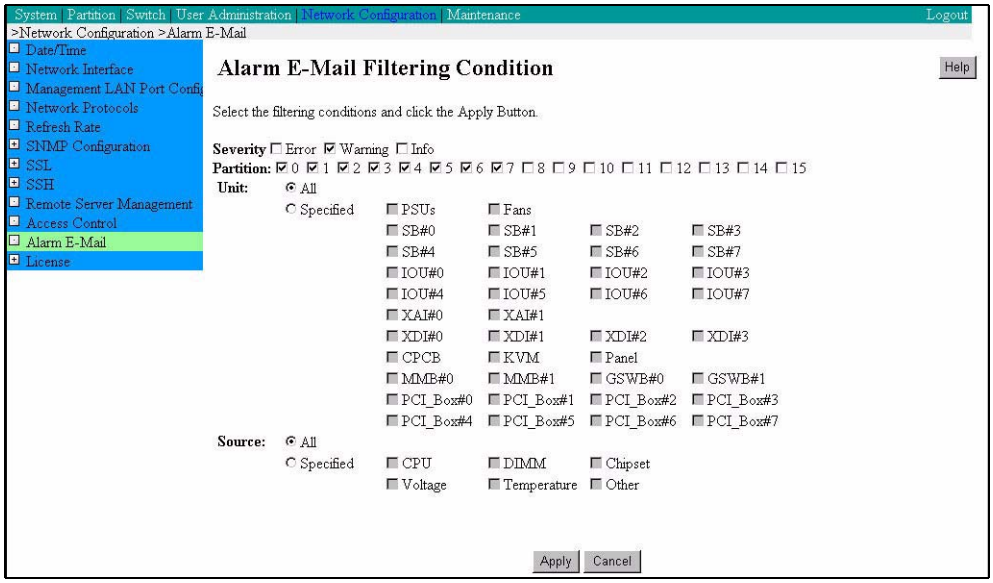


Abbildung 2.13 Das Fenster [Alarm E-Mail Filtering Condition] (PRIMEQUEST 580A/540A*/580/540/480/440)

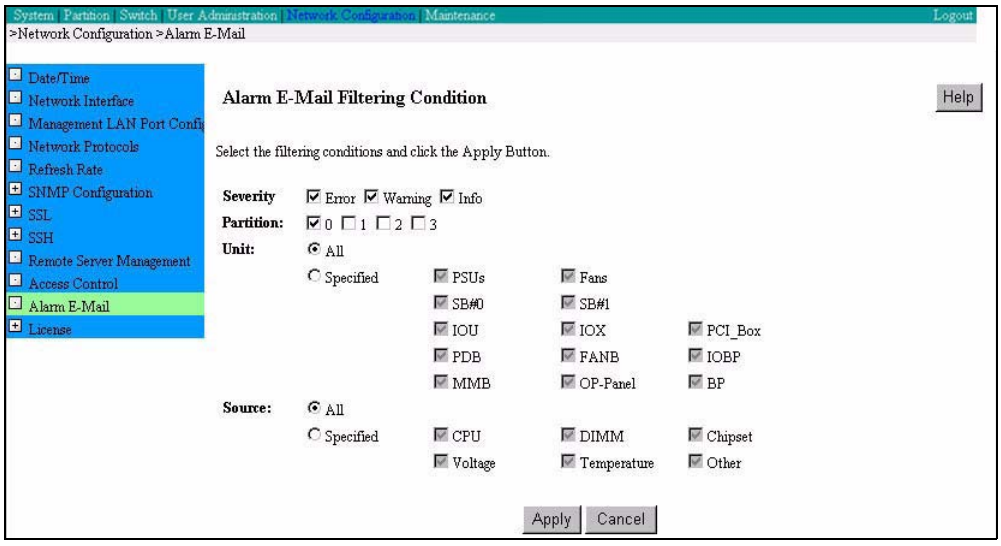


Abbildung 2.14 Das Fenster [Alarm E-Mail Filtering Condition] (PRIMEQUEST 520A*/520/420)

*: wird von Fujitsu Technology Solutions nicht unterstützt

2 Wählen Sie die gewünschten Positionen aus.
Wenn Sie mehrere Positionen auswählen, werden diese mit logischem AND verknüpft und die nachgeordneten Positionen mit logischem OR.

Tabelle 2.9 Feldnamen und mögliche Eingaben im Fenster [Alarm E-mail Filtering Condition]

Feldname	Beschreibung
Severity	Bestimmt den Schweregrad der Fehler, die per E-Mail gemeldet werden. Es kann mehr als ein Wert gewählt werden. • [Error]: Schwerwiegende Fehler wie beispielsweise Hardwareausfälle. • [Warning]: Ereignisse, die möglicherweise in der Zukunft zu Problemen führen können. • [Info]: Normale Systemereignisse wie das Einschalten einer Partition. Voreinstellung: Alle Kategorien
Partition	Bestimmt die Zielpartition, an die E-Mails gesendet werden. Es können mehrere Ziele angegeben werden. Voreinstellung: Alle Partitionen
Unit	Bestimmt die Einheiten, für die Ereignisse berichtet werden. Aktivieren Sie entweder [All] oder [Specified]. • Wenn Sie [All] aktivieren, werden Ereignisse von allen Einheiten gemeldet. • Wenn Sie [Specified] wählen, können Sie die Einheiten bestimmen, für die Ereignisse gemeldet werden. Klicken Sie das Kontrollkästchen vor einer Einheit an, um diese auszuwählen. Voreinstellung: [All]
Source	Bestimmen Sie die Quelle, für die E-Mail-Meldungen gemacht werden sollen. Aktivieren Sie entweder [All] oder [Specified]. • [All]: Ereignisse von allen Quellen werden gemeldet. • [Specified]: Sie können die Quellen auswählen.

3 Klicken Sie auf [Apply], um die gemachten Einstellungen zu übernehmen.

2.2.4 MMB initialisieren

In diesem Abschnitt wird beschrieben, wie Sie das MMB initialisieren.

Hinweis: Das MMB benutzt die folgenden TCP/IP-Portnummern:
- 623/udp: RMCP-Kommunikation
- 664/udp: RMCP-Kommunikation
- 5000: Ereignismitteilung vom PSA

Es wird empfohlen, die Einstellungen zu sichern, nachdem die im Folgenden beschriebenen Aufgaben durchgeführt wurden.

Wie Sie die Einstellungen sichern ist in Abschnitt 2.6, „Konfiguration sichern“, beschrieben.

- Benutzerkonten registrieren (→ 2.2.4.1)
- Benutzerkonto für den Techniker einrichten (→ 2.2.4.2)
- Systemnamen festlegen (→ 2.2.4.3)
- Systemdatum und Uhrzeit einstellen (→ 2.2.4.4)
- Einen Management-LAN-Hub einrichten (→ 2.2.4.5)

2.2.4.1 Benutzerkonten registrieren

Registrieren Sie die erforderlichen MMB-Benutzerkonten.

Vorgehensweise

1 Wählen Sie [User Administration] → [User List].
Das Fenster [User List] wird angezeigt.

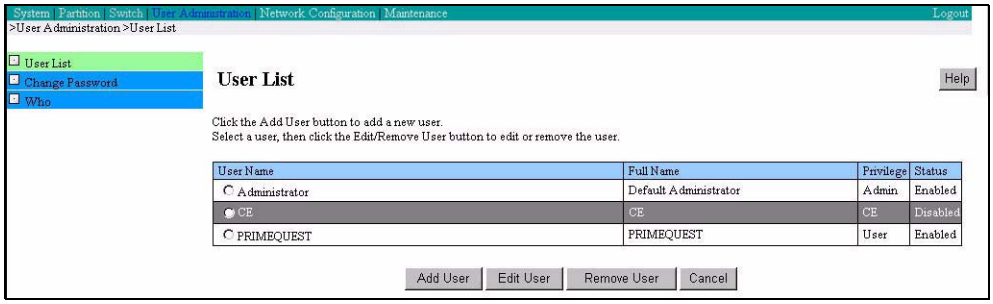


Abbildung 2.15 Das Fenster [User List]

Tabelle 2.10 Feldnamen und mögliche Eingaben im Fenster [User List]

Feldname	Beschreibung
User name	Name des Benutzers
Full Name	Name des Kontoinhabers
Privilege	Berechtigungen des Benutzers
Status	Aktueller Status des Benutzerkontos: aktiviert (Enabled) oder deaktiviert (Disabled).

2 Klicken Sie auf die Schaltfläche [Add User].
Das Fenster [Add User] wird angezeigt.

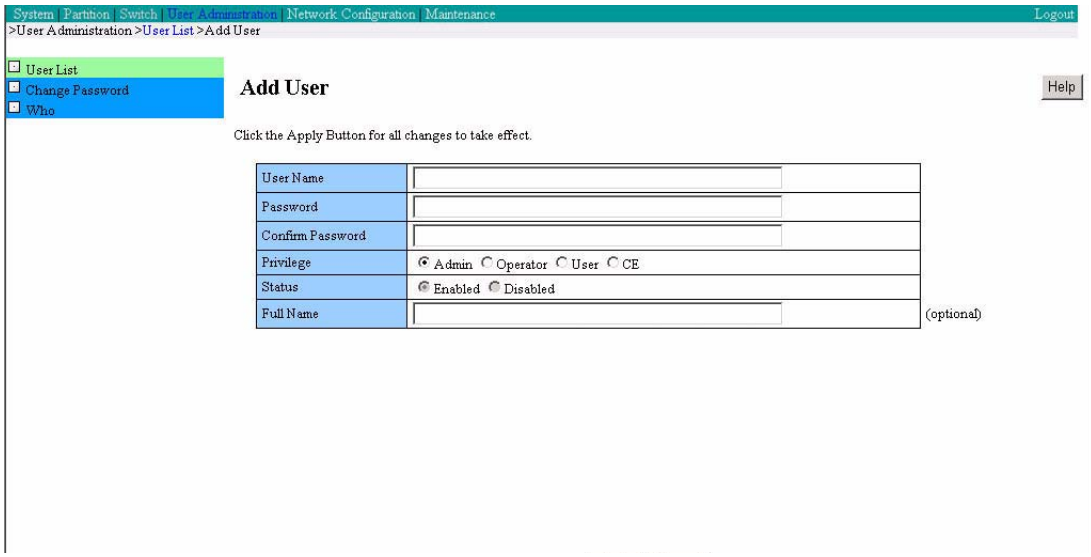


Abbildung 2.16 Das Fenster [Add User]

Anm.: Klicken Sie im Fenster [User List] auf die Schaltfläche [Edit User] und machen Sie im Fenster [Edit User] die erforderlichen Eingaben, wenn Sie ein bestehendes Benutzerkonto ändern wollen.

3 Machen Sie die erforderlichen Eingaben.

Tabelle 2.11 Feldnamen und mögliche Eingaben im Fenster [Add User]

Feldname	Beschreibung
User name	Geben Sie einen Benutzernamen ein (8 bis 32 Zeichen). Es sind die Zeichen 0 bis 9, a bis z, A bis Z sowie - und _ gestattet. Der Benutzername muss mit einem Buchstaben beginnen (groß oder klein).
Password	Geben Sie ein Kennwort ein (8 bis 32 Zeichen). Das Kennwort sollte nicht mithilfe eines Wörterbuchs leicht zu ermitteln sein. Wenn das Kennwort nicht zulässig ist, werden Sie aufgefordert, ein anderes zu wählen. Es sind die folgenden Zeichen zugelassen: Ziffern: 0 bis 9 Buchstaben: a bis z, A bis Z Sonderzeichen:! " # $ % & ' ( ) = - ^ ~ \ @ `[ ] { } : * ; + ? < . > , / _ |
Confirm Password	Wiederholen Sie die Eingabe des Kennworts zur Bestätigung.

Tabelle 2.11 Feldnamen und mögliche Eingaben im Fenster [Add User]

Feldname	Beschreibung	
Privilege	Legen Sie die Berechtigungen für das Benutzerkonto fest.	
	[User]	Der Benutzer verfügt nur über Leseberechtigung des PRIMEQUEST Systemstatus. Der Benutzer ist nicht berechtigt, die Systemkonfiguration zu ändern oder eine Partition ein- oder auszuschalten.
	[CE]	Der Benutzer ist berechtigt, den PRIMEQUEST Systemstatus zu lesen. Er ist nicht berechtigt, die Benutzerverwaltung oder Netzwerkkonfiguration betreffende Aufgaben durchzuführen oder eine Partition oder das System ein- oder auszuschalten. Der Benutzer kann Wartungsaufgaben durchführen.
	[Operator]	Der Benutzer ist berechtigt, den PRIMEQUEST Systemstatus zu lesen und ändern. Er ist jedoch nicht berechtigt, die Benutzerverwaltung oder die LAN-Konfiguration zu ändern.
	[Admin]	Der Benutzer ist berechtigt, sämtliche Aufgaben durchzuführen. Anm.: [Admin] bedeutet Administrator-Privilegien.
Status	Geben Sie den aktuellen Status des Kontos an. • [Enabled]: Das Benutzerkonto ist aktiviert. • [Disabled]: Das Benutzerkonto ist nicht aktiviert.	
Full Name	Hier kann der Name des Kontobesitzers oder andere Informationen eingegeben werden. Maximale Eingabelänge: 32 Zeichen.	

4 Klicken Sie auf [Apply], um die Eingaben zu übernehmen.

2.2.4.2 Benutzerkonto für den Techniker einrichten

Richten Sie ein Benutzerkonto ein, das der Kundendienst-Techniker für Wartungsarbeiten benutzen kann. Dazu gehen Sie vor wie bereits in Abschnitt 2.2.4.1, „Benutzerkonten registrieren“, beschrieben. Weisen Sie dem Benutzerkonto die Kontoberechtigung CE (Certified Engineer) zu.

2.2.4.3 Systemnamen festlegen

Geben Sie einen Namen für die PRIMEQUEST ein. Dies kann nur von Benutzern mit Systemverwalterrechten (Admin) durchgeführt werden. Der Systemname wird auch als SNMP-Systemname benutzt.

Vorgehensweise

1 Wählen Sie [System] → [System Information].
Das Fenster [System Information] wird angezeigt.

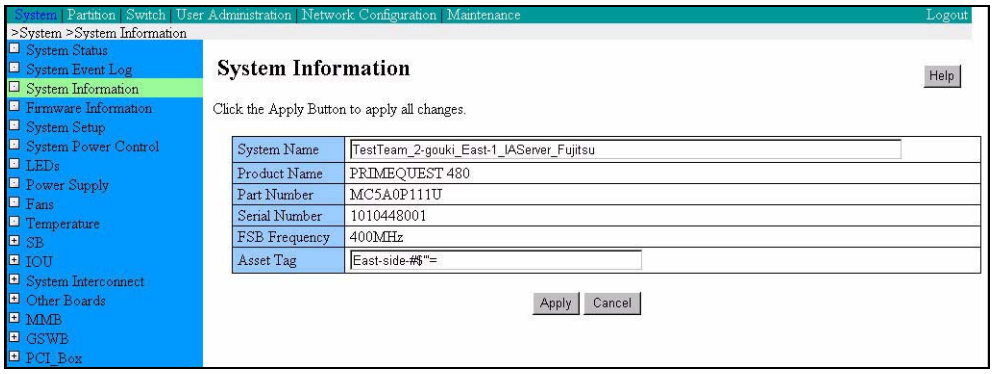


Abbildung 2.17 Das Fenster [System Information]

2 Geben Sie im Feld [System Name] einen Rechnernamen ein.

Tabelle 2.12 Feldnamen und mögliche Eingaben im Fenster [System Information]

Feldname	Beschreibung
System Name	Der der PRIMEQUEST zugewiesene Name wird angezeigt. Benutzer mit Systemverwalterrechten können diesen Namen ändern. Der Systemname kann maximal 64 Zeichen lang sein. Voreinstellung: PRIMEQUEST + Seriennummer Anm.: • Jedes der folgenden Zeichen kann verwendet werden: [0-9],[a-z],[A-Z], (n-Leerzeichen) ! " # $ % & ' ( ) = - ^ ~ \ @ ` [ ] { } : * ; + ? < . > , / _ | Es gelten folgende Restriktionen: - Am Beginn des Strings darf eines der folgenden Zeichen nicht stehen: # (n-Leerzeichen) - Am Beginn des Strings darf das folgende Zeichen nicht stehen: (n-Leerzeichen) • Dieser Name wird auch als SNMP-Systemname benutzt. Ein separater SNMP-Systemname kann nicht festgelegt werden. Der hier festgelegte Name erscheint auch im Fenster [SNMP Configuration] und kann dort nicht geändert werden.
Product Name	Produktname des PRIMEQUEST Systems
Part Number	Teilenummer des PRIMEQUEST Systems Anm.:Nehmen Sie Kontakt zu einem Kundendienst-Techniker auf, wenn „Read Error“ angezeigt wird.
Serial Number	Seriennummer des PRIMEQUEST Systems Anm.:Nehmen Sie Kontakt zu einem Kundendienst-Techniker auf, wenn „Read Error“ angezeigt wird.
FSB Frequency	Frequenz
Asset Tag	Informationen zur Anlagenverwaltung Der Systemverwalter ist berechtigt, diese Informationen zu ändern. Die maximale Feldlänge ist 32 Zeichen. Anm.:Mit diesem Feld wird Anwendern die Möglichkeit gegeben, die Anlagennummer u.ä. ihrer PRIMEQUEST zu verwalten.

3 Klicken Sie auf [Apply], um die Eingaben zu übernehmen.

2.2.4.4 Systemdatum und Uhrzeit einstellen

Stellen Sie das Datum und die Zeit des MMB und ggf. des NTP-Servers ein.

Dieser Schritt ist nicht erforderlich, wenn er bereits vom Kundendienst-Techniker zur Ausführung des Testprogramms durchgeführt wurde.

Anm.: Das MMB verfügt über NTP-Client- und -Serverfunktionen. Die Clientfunktion des MMB stellt die Zeit mithilfe des anderen NTP-Servers ein. Jede Partition der PRIMEQUEST benutzt die NTP-Serverfunktion des MMB, um ihre Zeit genau einzustellen.
Das MMB braucht jedoch für den NTP-Server nicht in irgendeiner der Partitionen spezifiziert zu werden. Geben Sie auf dem NTP-Client mehrere NTP-Server an (es werden wenigstens drei empfohlen).

Vorgehensweise

1 Wählen Sie [Network Configuration] → [Date/Time].
Das Fenster [Date/Time], in dem Sie Datum und Zeit einstellen können, wird angezeit.

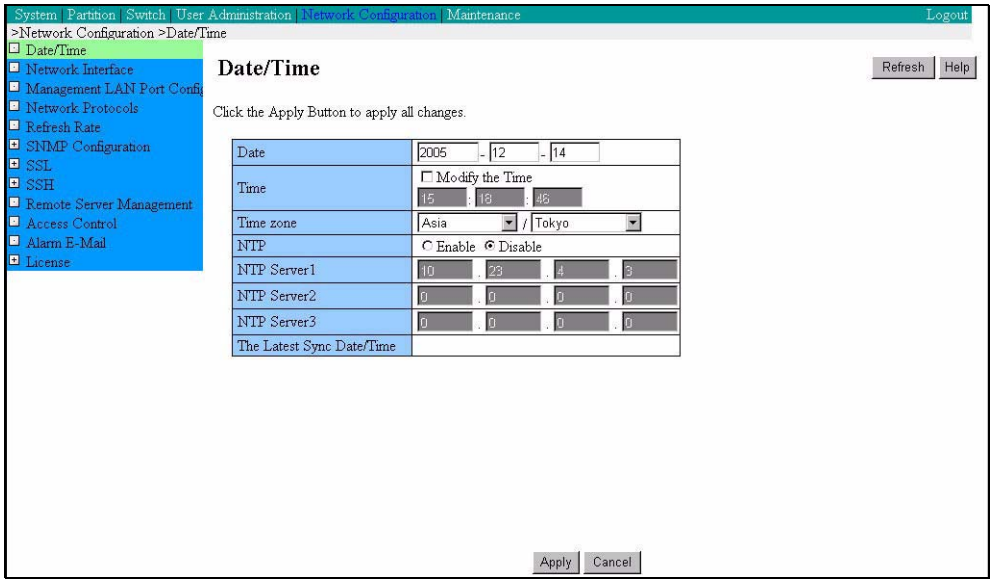


Abbildung 2.18 Das Fenster [Date/Time]

2 Machen Sie die erforderlichen Eingaben.

Tabelle 2.13 Feldnamen und mögliche Eingaben im Fenster [Date/Time]

Feldname	Beschreibung
Date	Zeigt das Datum an. * Bei Verwendung eines NTP-Server keine Eingabe nötig.
Time	Uhrzeit im Format hh:mm:ss. Aktivieren Sie das Kontrollkästchen [Modify the Time], um die Uhrzeit einstellen zu können. Da hier beim Öffnen des Fensters die MMB-Zeit angezeigt wird, ist zur Aktualisierung der Anzeige ein Reload erforderlich. Wenn die Zeit automatisch aktualisiert wird, zeigt dieses Feld die Uhrzeit an, zu der das Fenster geöffnet wurde. * Bei Verwendung eines NTP-Server keine Eingabe nötig.
Time zone	Wählen Sie aus dem Pulldown-Menü eine Zeitzone aus.
NTP	NTP-Funktion aktivieren bzw. deaktivieren (Enable/Disable). Wenn die NTP-Funktion aktiviert ist, synchronisiert das MMB die Zeit mit der NTP-Serverzeit anhand der in den folgenden Feldern NTP Server1 bis NTP Server3 angegebenen Servern. Die NTP-Funktion muss aktiviert sein, wenn andere Clients, beispielsweise Partitionen, ihre Systemzeit anhand des MMBs synchronisieren. Voreinstellung: deaktiviert
NTP Server1	IP-Adresse des ersten NTP-Servers. (Gilt, wenn die NTP-Funktion aktiviert ist.)
NTP Server2	IP-Adresse des zweiten NTP-Servers. (Gilt, wenn die NTP-Funktion aktiviert ist.)
NTP Server3	IP-Adresse des dritten NTP-Servers. (Gilt, wenn die NTP-Funktion aktiviert ist.)
The Latest Sync Data/Time	Letzte Aktualisierung der MMB-Systemzeit durch den angegebenen NTP-Server.

3 Klicken Sie auf [Apply], um die Eingaben zu übernehmen.

2.2.4.5 Einen Management-LAN-Hub einrichten

Diese Funktion legt die Übertragungsgeschwindigkeit und den Duplexmodus für jeden Port eines MMB fest und richtet zwischen den LAN-Ports der Partition und des MMBs ein VLAN ein, das mit dem Management-LAN verbunden ist. Ferner wird für jeden MMB-Port die Übertragungsgeschwindigkeit und das Übertragungsverfahren (Vollduplex/Halbduplex) festgelegt. Für diese Einstellungen sind Systemverwalter-berechtigungen erforderlich

Geschwindigkeit-/Duplex-Einstellung für den Management-LAN-Port

Stellen Sie „AUTO“ für Speed/Duplex des USER-Ports ein.

Anmerkung: Falls der USER-Port anders als auf „AUTO“ eingestellt ist, ist die MDI/MDI-X-Funktion deaktiviert. Verwenden Sie zur Vermeidung dieses Problems die folgenden Kabel:
Verbindung zum Switching Hub: Crossover-Kabel
Direkte Verbindung zu einem PC: Straight-Kabel

Beachten Sie ebenfalls folgende Hinweise zum REMCS*-Port:

- PRIMEQUEST 500/400
  Der REMCS*-Port besitzt ebenfalls die Auto MDI-X-Funktion. Verwenden Sie hier das gleiche Kabel wie für den USER-Port, falls der REMCS*-Port nicht auf „AUTO“ eingestellt ist.
- PRIMEQUEST 580A/540A*/520A*
  - Der REMCS*-Port besitzt die Auto MDI-X-Funktion nicht. Verwenden Sie unabhängig von den Speed/Duplex-Einstellungen folgende Kabel:
    Verbindung zum Switching Hub: Straight-Kabel
    Direkte Verbindung zu einem PC: Crossover-Kabel
    Achtung:
    Hier wird ein anderes Kabel als für den USER-Port verwendet.
  - Falls ein mit dem REMCS*-Port verbundenes Gerät bei Speed/Duplex auf einen anderen Wert als „AUTO“ eingestellt ist, verwenden Sie für den REMCS*-Port unbedingt dieselbe Einstellung.

*: wird von Fujitsu Technology Solutions nicht unterstützt

VLAN-Funktionen des Management-LANs und VLAN-Mode

Im Management-LAN-Hub des MMBs befinden sich Partition-Netzwerke, Benutzerports, REMCS*-Ports und die Ports des Kundendienst-Technikers. Bei einem typischen Hub können die folgenden Probleme auftauchen:

- Die Kommunikation zwischen den Partitionen ist aktiviert, d.h. von einer Partition aus kann auf eine andere Partition zugegriffen werden, was ein Sicherheitsrisiko darstellt.
- Auf das Transaktionssystem eines Benutzers kann vom REMCS*-Port und vom Port des Kundendienst-Technikers aus zugegriffen werden.

Im Management-LAN-Hub kommen daher VLANs zum Einsatz, um diese Sicherheitsrisiken zu beseitigen. Mit einem VLAN wird jeder Port eines Switching Hubs logisch in Gruppen untergliedert, die jeweils als unabhängige LANs fungieren.

Die VLAN-Funktionen eines PRIMEQUEST Management-LANs können nach einer der drei im Folgenden beschriebenen Verfahren betrieben werden.

Es stehen drei verschiedene Verfahren für den Betrieb des Management-LANs zur Verfügung. Dabei ist der VLAN-Modus als Standardverfahren zu betrachten.

- Kein VLAN-Modus (Kommunikation zwischen den Partitionen ist zugelassen)
  - Kommunikation zwischen den Ports aller Partitionen ist zugelassen.
  - Kommunikation zwischen den REMCS*-Ports, den Ports der Kundendienst-Techniker und den Benutzerports sowie die Kommunikation zwischen den REMCS*-Ports, den Ports der Kundendienst-Techniker und den Partitionsports ist nicht zugelassen. (Tabelle 2.14).
- VLAN-Modus (Kommunikation zwischen den Partitionen ist nicht zugelassen)
  - Die Kommunikation zwischen den Partitionen ist nicht zugelassen. Die Kommunikation zwischen einem Benutzerports und einem Partitionsport sowie zwischen dem MMB und einer Partition im PRIMEQUEST-Schrank ist zugelassen. Kommunikation ist nur zwischen Ports möglich, bei denen in der Tabelle 2.15 „Y“ angegeben ist.
    Zwischen dem Benutzerport, dem MMB und den Partitionsports ist eine Kommunikation zugelassen.
- Port Disable-Modus (Kommunikation zwischen Partitionen und Management-LAN deaktiviert)
  - Modus für höhere Sicherheitsstufen

*: wird von Fujitsu Technology Solutions nicht unterstützt

- Die Ports sämtlicher Partitionen sind gesperrt. Eine Kommunikation zwischen dem Management-LAN und den Partitionsports ist nicht möglich. Eine Kommunikation ist nur zwischen den Ports möglich, die in Tabelle 2.16 auf „Y“ gesetzt sind.
  Es ist keine Kommunikation zwischen dem MMB und einem beliebigen Partitionsport möglich.

Tabelle 2.14 Aktivierte Ports in einem Management-LAN ohne VLAN-Modus

Kein VLAN-Modus	Benutzer	Kundendienst-Techniker	REMCS*-Ports	MMB	Partitionsports
Benutzer	Y	N	N	Y	Y
Kundendienst-Techniker	N	Y	N	Y	N
REMCS*-Ports	N	N	Y	Y	N
MMB	Y	Y	Y	Y	Y
Partitionsports	Y	N	N	Y	Y

Y: Kommunikation aktiviert
N: Kommunikation deaktiviert
*: wird von Fujitsu Technology Solutions nicht unterstützt

Tabelle 2.15 Aktivierte Ports in einem Management-LAN mit VLAN-Modus 1

VLAN-Modus	Benutzer	Kundendienst-Techniker	REMCS*-Ports	MMB	Partitionsports
Benutzer	Y	N	N	Y	Y
Kundendienst-Techniker	N	Y	N	Y	N
REMCS*-Ports	N	N	Y	Y	N
MMB	Y	Y	Y	Y	Y
Partitionsports	Y	N	N	Y	N

Y: Kommunikation aktiviert
N: Kommunikation deaktiviert
*: wird von Fujitsu Technology Solutions nicht unterstützt

Tabelle 2.16 Aktivierte Ports in einem Management-LAN im Port Disable-Modus

Port Disable-Modus	Benutzer	Kundendienst-Techniker	REMCS*-Ports	MMB	Partitionsports
Benutzer	Y	N	N	Y	N
Kundendienst-Techniker	N	Y	N	Y	N
REMCS*-Ports	N	N	Y	Y	N
MMB	Y	Y	Y	Y	N
Partitionsports	N	N	N	N	N

Y: Kommunikation aktiviert
N: Kommunikation deaktiviert
*: wird von Fujitsu Technology Solutions nicht unterstützt

Vorgehensweise

1 Wählen Sie [Network Configuration] → [Management LAN Port Configuration]. Das Fenster [Management LAN Port Configuration] wird angezeigt.

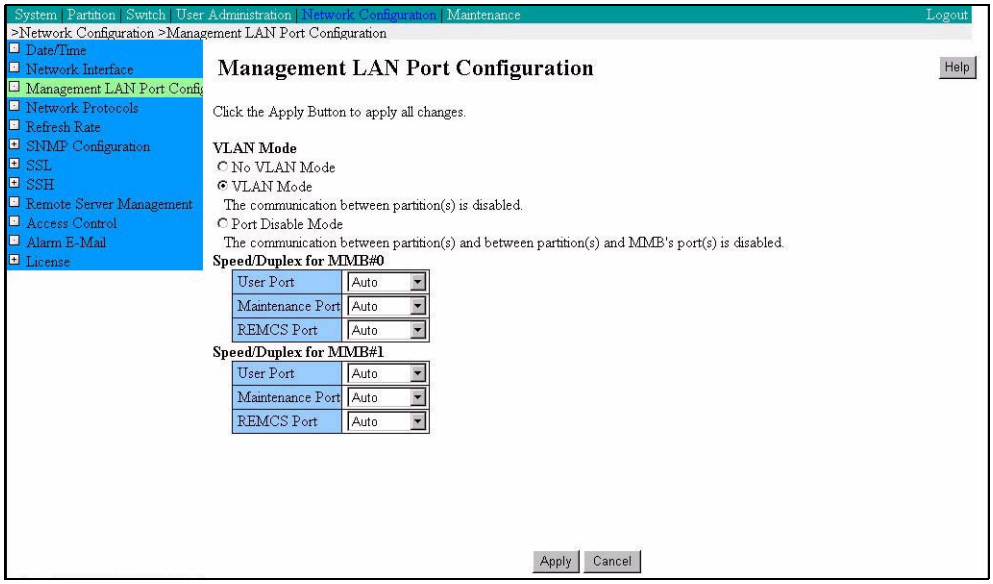


Abbildung 2.19 Das Fenster [Management LAN Port Configuration] (PRIMEQUEST 580A/540A*/580/540/480/440)

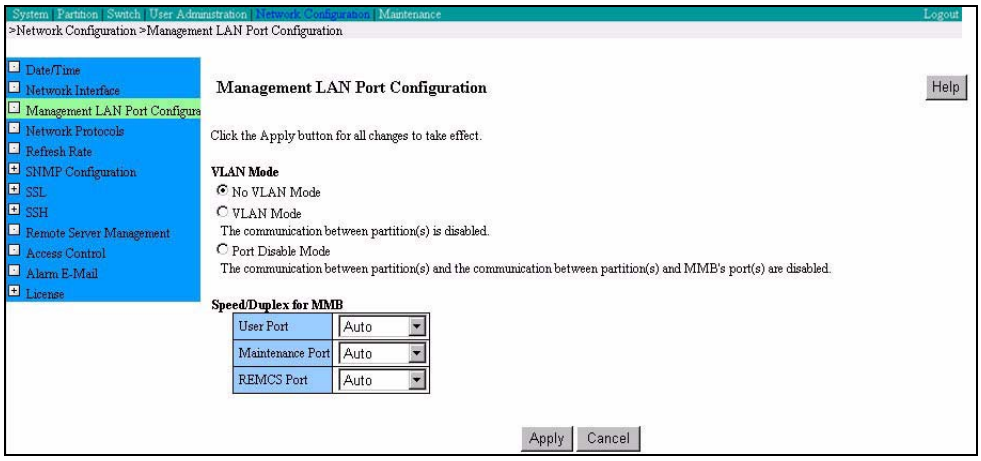


Abbildung 2.20 Das Fenster [Management LAN Port Configuration] (PRIMEQUEST 520A*/520/420)

2 Geben Sie die erforderlichen Daten ein.

*: wird von Fujitsu Technology Solutions nicht unterstützt

Tabelle 2.17 Feldnamen und mögliche Eingaben im Fenster [Management LAN Port Configuration]

Feldname	Beschreibung
VLAN Mode	Legt den VLAN-Modus für den MMB-Hub fest. • [No VLAN Mode]: Aktiviert die Kommunikation zwischen den MMB-Ports und allen Partitionsports. • [VLAN mode]: Deaktiviert die Kommunikation zwischen den Partitionen. • [Port disable mode]: deaktiviert die Kommunikation zwischen den Partitionen sowie zwischen den MMB-Ports und den Partitionen. Voreinstellung: [VLAN-Modus]
Speed/Duplex for MMB (PRIMEQUEST 520A*/520/420)	Legt Übertragungsgeschwindigkeit/-verfahren für das MMB fest. • [Auto]: Automatische Einstellung • [100M/Full]: Vollduplex mit 100 Mbps • [100M/Half]: Halbduplex mit 100 Mbps • [10M/Full]: Vollduplex mit 10 Mbps • [10M/Half]: Halbduplex mit 10 Mbps Voreinstellung: [Auto]
Speed/Duplex for MMB#0 (PRIMEQUEST 580A/540A*/580/540/480/440)	Legt Übertragungsgeschwindigkeit/-verfahren für MMB#0 fest. • [Auto]: Automatische Einstellung • [100M/Full]: Vollduplex mit 100 Mbps • [100M/Half]: Halbduplex mit 100 Mbps • [10M/Full]: Vollduplex mit 10 Mbps • [10M/Half]: Halbduplex mit 10 Mbps Hinweis: Wird nur bei Installation von MMB#0 angezeigt. Voreinstellung: [Auto]
Speed/Duplex for MMB#1 (PRIMEQUEST 580A/540A*/580/540/480/440)	Legt Übertragungsgeschwindigkeit/-verfahren für MMB#1 fest. • [Auto]: Automatische Einstellung • [100M/Full]: Vollduplex mit 100 Mbps • [100M/Half]: Halbduplex mit 100 Mbps • [10M/Full]: Vollduplex mit 10 Mbps • [10M/Half]: Halbduplex mit 10 Mbps Hinweis: Wird nur bei Installation von MMB#1 angezeigt. Voreinstellung: [Auto]

*: wird von Fujitsu Technology Solutions nicht unterstützt

3 Klicken Sie auf [Apply], um die Eingaben zu übernehmen.

2.3 Extended Mirror Mode aktivieren

Damit Sie eine Partition im Extended Mirror Mode (erweiterten Spiegelmodus) betreiben können, müssen Sie eine System Mirror Option erwerben, und die Lizenzdaten müssen registriert sein.

Möglicherweise wurde der Extended Mirror Mode bereits im Werk vor der Auslieferung Ihres Systems aktiviert. In diesem Fall erübrigt sich dieser Einstellvorgang. Klären Sie Einzelheiten mit einem Kundendienst-Techniker.

1 Legen Sie die zum Lieferumfang der System Mirror Option gehörende CD-ROM in das CD-ROM-Laufwerk der MMB-Konsole ein.

2 Wählen Sie [Network Configuration] → [License] → [Mirror License].
Das Fenster [Mirror License] wird angezeigt.

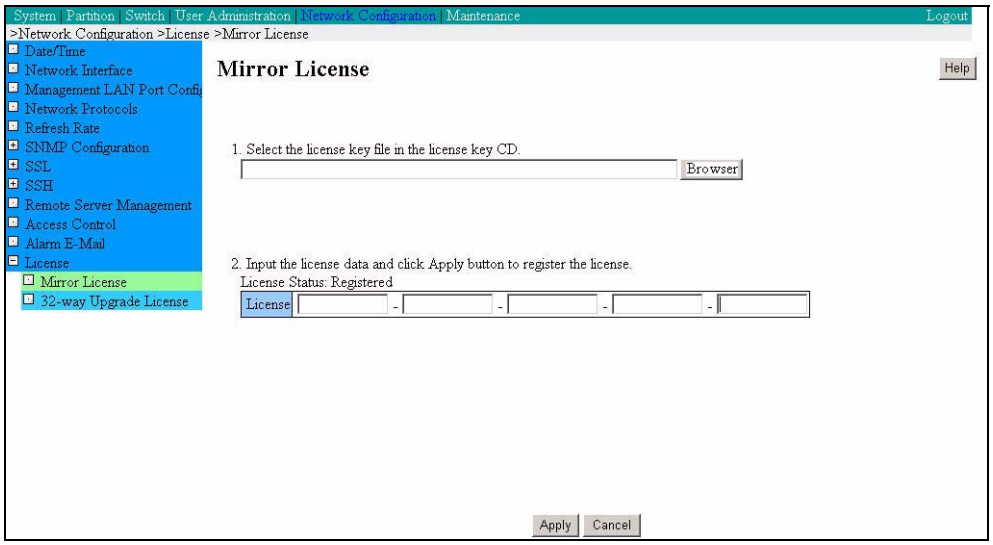


Abbildung 2.21 Das Fenster [Mirror License]

Tabelle 2.18 Feldnamen und mögliche Eingaben im Fenster [Mirror License]

Feldname	Beschreibung
Select the license key file in the license key CD.	Wählen Sie die Lizenzschlüsseldatei aus, mit der die Lizenz validiert wird.
License Status	Zeigt den aktuellen Status der Lizenz an. • Not registered: Die Lizenz ist nicht registriert. Oder die für die Registrierung (eingegebenen) Lizenzdaten sind nicht zutreffend. • Registered: Die Lizenz ist registriert.
License	Geben Sie die Lizenzdaten ein.

3 Klicken Sie auf die Schaltfläche [Browse] und wählen Sie im Dateiauswahlfenster die Lizenzschlüsseldatei aus.

4 Geben Sie im Feld [License] die Lizenzdaten vom Schreiben ein, das zum Lieferumfang der System Mirror Option gehört, und klicken Sie dann auf die Schaltfläche [Apply].
Nun kann die Option Extended Mirror Mode in jeder Partition gesetzt werden.

Anm.: Näheres darüber, wie Sie den Extended Mirror Mode einstellen, finden Sie in 2.5.8, „Verschiedene Modes einstellen“.

Hinweis: Die System Mirror Option muss zusätzlich zur PRIMEQUEST Systemeinheit erworben werden.

2.4 XPAR aktivieren (PRIMEQUEST 500A/500 Modellreihe)

Für den Betrieb geteilter Systemboards, IO Units und IOXs, die in Partitionen eingesetzt werden, muß eine XPAR-Option beschafft und eine Lizenz registriert werden.

Möglicherweise wurde die XPAR-Option bereits im Werk vor der Auslieferung Ihres Systems aktiviert. In diesem Fall erübrigt sich dieser Einstellvorgang.

Klären Sie Einzelheiten mit einem Kundendienst-Techniker.

1 Legen Sie in das CD-ROM-Laufwerk der MMB-Konsole die mit der XPAR-Option gelieferte CD-ROM ein.

2 Klicken Sie [Network Configuration] → [License] → [XPAR License].
Das Fenster [XPAR License] wird angezeigt.

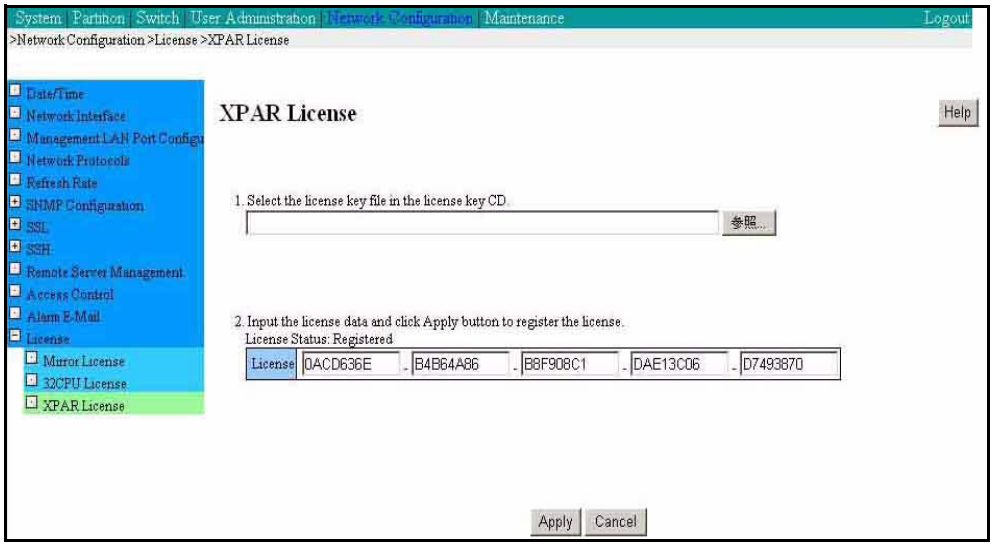


Abbildung 2.22 Fenster [XPAR License]

Tabelle 2.19 Feldnamen und mögliche Eingaben im Fenster [XPAR License]

Feldname	Beschreibung
Select the license key file in the license key CD.	Wählen Sie die Lizenzschlüsseldatei aus, mit der die Lizenz validiert wird.
License Status	Zeigt den aktuellen Status der Lizenz an. • Not registered: Die Lizenz ist nicht registriert. Oder die für die Registrierung (eingegebenen) Lizenzdaten sind nicht zutreffend. • Registered: Die Lizenz ist registriert.
License	Geben Sie die Lizenzdaten ein.

3 Klicken Sie auf die Schaltfläche [Browse] und wählen Sie im Dateiauswahlfenster die Lizenzschlüsseldatei aus.

4 Geben Sie im Feld [License] die Lizenzdaten vom Schreiben ein, das zum Lieferumfang der XPAR-Option gehört, und klicken Sie dann auf die Schaltfläche [Apply].
Nun kann die XPAR-Option in jeder Partition gesetzt werden.

Anm.: Näheres darüber, wie Sie die XPAR-Option einstellen, finden Sie in Abschnitt 2.5.3, „Systemboards, IO Units und IOXs teilen und wieder verbinden (nur in der Modellreihe PRIMEQUEST 500A/500)“.

Hinweis: Die XPAR-Option muss zusätzlich zur PRIMEQUEST Systemeinheit erworben werden.

2.5 Partition initialisieren

In diesem Abschnitt wird beschrieben, wie Sie die verschiedenen Angaben zu den Partitionen festlegen. Die Schritte müssen für jede Partition durchgeführt werden.

Folgende Aufgaben werden beschrieben:

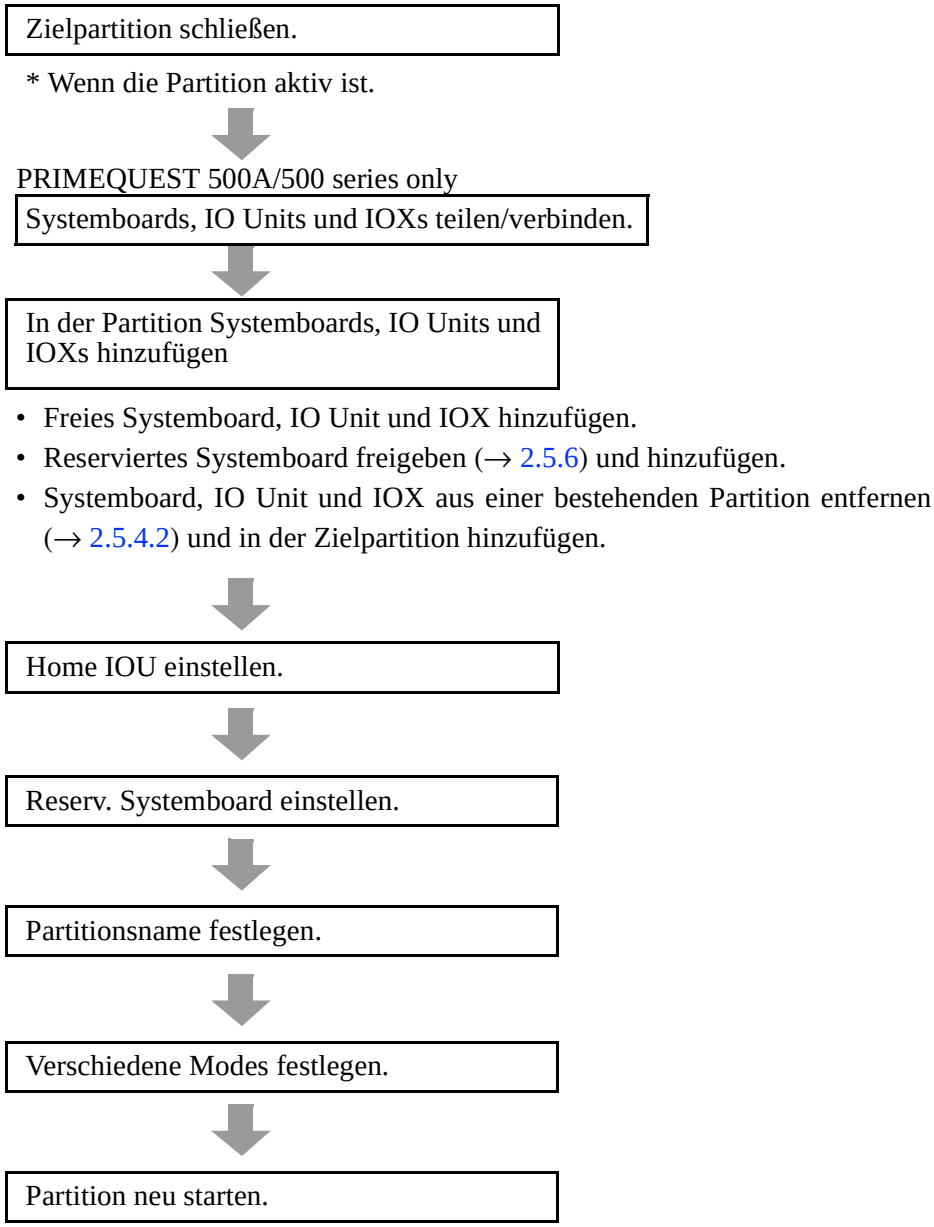
- Reihenfolge der Einstellungen (→ 2.5.1)
- Partition schließen (→ 2.5.2)
- Systemboards, IO Units und IOXs teilen und wieder verbinden (nur in der Modellreihe PRIMEQUEST 500A/500) (→ 2.5.3)
- Systemboards, IO Units und IOXs hinzufügen (→ 2.5.4.1)
- Systemboards, IO Units und IOXs entfernen (→ 2.5.4.2)
- Home IO Unit festlegen (→ 2.5.5)
- Systemboard reservieren (→ 2.5.6)
- Partitionsnamen festlegen (→ 2.5.7)
- Verschiedene Modes einstellen (→ 2.5.8)
- Partition starten (→ 2.5.9)
- Partitionsinformationen anzeigen (→ 2.5.10)

2.5.1 Reihenfolge der Einstellungen

Folgen Sie für jede Partition, die Sie einrichten wollen, dem in der folgenden Übersicht angegebenen Arbeitsablauf. Bei den einzelnen Schritten werden als Beispiel Bildschirmabzüge der Systeme PRIMEQUEST 580A/540A*/580/540/480/440 verwendet.

Hinweis: Wenn Sie die Konfiguration einer aktiven Partition ändern, muss diese geschlossen und neu gestartet werden, damit die Änderungen wirksam werden.

*: wird von Fujitsu Technology Solutions nicht unterstützt


Zielpartition schließen.
* Wenn die Partition aktiv ist.
PRIMEQUEST 500A/500 series only
Systemboards, IO Units und IOXs teilen/verbinden.
In der Partition Systemboards, IO Units und IOXs hinzufügen
• Freies Systemboard, IO Unit und IOX hinzufügen.
• Reserviertes Systemboard freigeben (→ 2.5.6) und hinzufügen.
• Systemboard, IO Unit und IOX aus einer bestehenden Partition entfernen (→ 2.5.4.2) und in der Zielpartition hinzufügen.
Home IOU einstellen.
Reserv. Systemboard einstellen.
Partitionsname festlegen.
Verschiedene Modes festlegen.
Partition neu starten.

2.5.2 Partition schließen

Dieser Abschnitt beschreibt, wie Sie vorgehen müssen, um eine aktive Partition zu schließen.

Vorgehensweise

1 Klicken Sie [Partition] → [Power Control].
Das Fenster [Power Control] wird angezeigt.

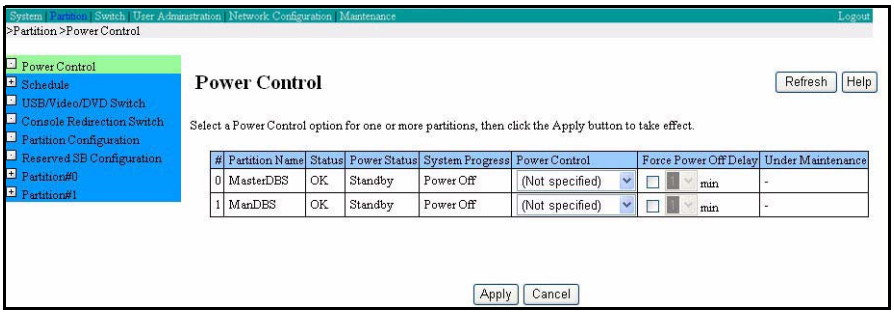

System | Partition | Switch | User Administration | Network Configuration | Maintenance
Logout
>Partition >Power Control
Power Control
Schedule
USB/Video/DVD Switch
Console Redirection Switch
Partition Configuration
Reserved SB Configuration
Partition#0
Partition#1
Power Control
Refresh
Help
Select a Power Control option for one or more partitions, then click the Apply button to take effect.
Partition Name Status Power Status System Progress Power Control Force Power Off Delay Under Maintenance
0 MasterDBS OK Standby Power Off (Not specified) min -
1 ManDBS OK Standby Power Off (Not specified) min -
Apply
Cancel

Abbildung 2.23 Das Fenster [Power Control]

2 Wählen Sie im Fenster [Power Control] für die betreffende Partition [Power off] und klicken Sie dann auf die Schaltfläche [Apply].

Anmerkung: Möglicherweise können Sie eine Partition, in der Windows installiert ist, nicht vom MMB Web-UI schließen. Führen Sie in diesem Fall das Shutdown-Kommando von Windows aus. Einzelheiten finden Sie in der Windows-Dokumentation oder im *PRIMEQUEST 580A/540A/520A/500/400 Series Reference Manual: Basic Operation/GUI/Commands* (U41633-J-Z816-x-76/C122-E003EN).

Tabelle 2.20 Feldnamen und mögliche Eingaben im Fenster [Power Control]

Feld	Beschreibung
Power Control	Wählen Sie die Power Control-Einstellung für die Partition aus. Der Option [Power On] wird für eine eingeschaltete Partition nicht angeboten. Umgekehrt werden die Optionen [Power Off], [Power Cycle], [Reset], [INIT], und [Force Power Off] für ausgeschaltete Partitionen nicht angeboten. • Power On: Schaltet die Partition ein. • Power Off: Schaltet die Partition aus. • Power Cycle: Erzwingt das Aus- und wieder Einschalten der Partition. • Reset: Setzt die Partition zurück. • INIT: Erzeugt für die Partition ein INIT und ein Dump. • Force Power Off: Erzwingt das Ausschalten der Partition. • Not specified: Es wird für die Partition keine Aktion ausgeführt. Anm.: • Führen Sie ein INIT aus, um das Beenden von in der Partition ablaufenden Anwendungen zu erzwingen. Schließen Sie wichtige Anwendungen, bevor Sie ein INIT ausführen. Hängen Sie ferner nicht benötigte Dateisysteme vor einem INIT aus.

2.5.3 Systemboards, IO Units und IOXs teilen und wieder verbinden (nur in der Modellreihe PRIMEQUEST 500A*/500)

In der Modellreihe PRIMEQUEST 500A*/500 können Sie je nach Bedarf Systemboards, IO Units und IOXs logisch in zwei separate Einheiten teilen, um in der Systemkonfiguration flexibel zu sein.

Dieser Abschnitt beschreibt das Vorgehen beim Teilen und Wiederverbinden von Systemboards, IO Units und IOXs.

Anmerkung: Systemboards, IO Unit und IOXs, die zu einer Partition gehören, die im Extended Mirror Mode arbeitet, können nicht geteilt werden.

Sie könne nur freie Systemboards, IO Units und IOXs teilen oder wieder verbinden. Um Systemboards, IO Units und IOXs, die zu einer Partition gehören, teilen oder wieder verbinden zu können, müssen diese jeweils zuerst aus Ihrer Partition auskonfiguriert werden.

Hinweise:

- Falls die XPAR-Lizenz noch nicht registriert wurde, werden das Menü [Split Configuration] sowie die Fenster [SB Split] und [IOU Split] nicht angezeigt.
- Der Extended Mirror Mode kann nicht in Partitionen aktiviert werden, die Systemboards, IO Units oder IOXs enthalten, die mit XPAR geteilt wurden. Das Teilen von Systemboards, IO Units oder IOXs kann in Partitionen, in den der Extended Mirror Mode aktiviert ist, nicht durchgeführt werden.
- Ein Systemboard, das mit XPAR geteilt wurde, kann nicht als Systemboard für eine Partition reserviert werden, in der der Extended Mirror Mode aktiviert wurde.
  Der Extended Mirror Mode kann in Partitionen nicht aktiviert werden, für die geteilte Systemboards reserviert wurden.
- XPAR wird ausschließlich von der Modellreihe PRIMEQUEST 500A*/500 unterstützt, und die Beschaffung und Installation der XPAR-Option ist Voraussetzung für die Anwendung von XPAR.

2.5.3.1 Systemboards teilen und wieder verbinden

Dieser Abschnitt beschreibt das Vorgehen beim Teilen und Wiedererbinden von Systemboards.

Anmerkung: Falls die XPAR-Lizenz noch nicht registriert wurde, wird das Fenster [SB Split] nicht angezeigt.

*: wird von Fujitsu Technology Solutions nicht unterstützt

1 Klicken Sie [Partition] → [Split Configuration] → [SB Split].
Das Fenster [SB Split] wird angezeigt.

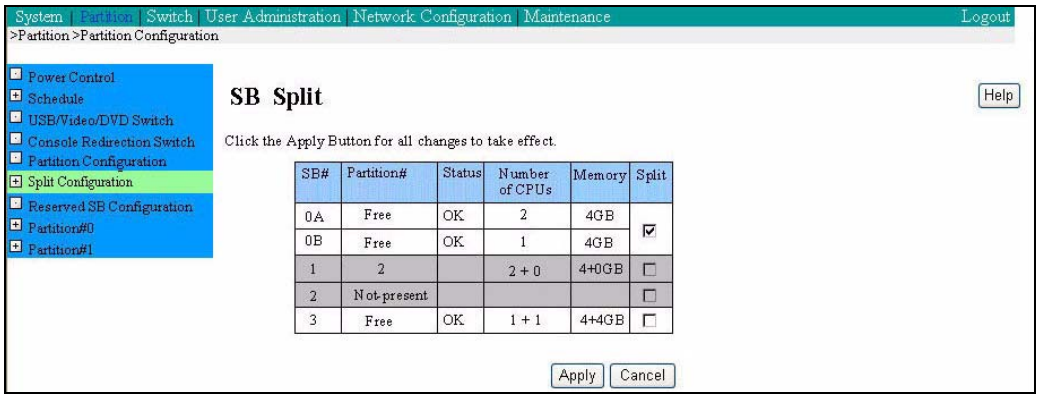


Abbildung 2.24 Fenster [SB Split]

Tabelle 2.21 Feldnamen und mögliche Eingaben im Fenster [SB Split]

Feld	Beschreibung
SB#	Anzeige der Systemboard-Identifikationsnummer (ggf. zwei). Falls das Systemboard bereits geteilt ist, werden xA und xB angezeigt.
Partition#	Anzeige der Partition-Nummer oder „Free“ (die Partition ist dann frei).
Status	Anzeige des Systemboard-Status.
Number of CPUs	Anzeige der Anzahl an CPUs auf dem Systemboard.
Memory	Anzeige des auf dem Systemboard verfügbaren Hauptspeichers.
Split	Kontrollkästchen zum Teilen/Wiederverbinden des Systemboards.

- Systemboard teilen:

  1 Aktivieren Sie das Kontrollkästchen [Split] des Systemboard, um es in zwei Einheiten zu teilen, und klicken Sie auf [Apply].
  Das Systemboard wird in zwei Einheiten geteilt, und im Fenster wird xA und xB angezeigt.

- Systemboards wieder verbinden:

  1 Deaktivieren Sie das Kontrollkästchen [Split] des Systemboard, dessen beide Teile wieder verbunden werden soll, und klicken Sie auf [Apply].
  Die Teile des Systemboard werden wieder verbunden und als ein Systemboard im Fenster angezeigt.

2.5.3.2 IO Units oder IOXs teilen und wieder verbinden

Dieser Abschnitt beschreibt das Vorgehen beim Teilen und Wiedererbinden von IO Units und IOXs. Nur freie IO Units und IOXs, die zu einer Partition gehören, können geteilt werden.

Anmerkung: Falls die XPAR-Lizenz noch nicht registriert wurde, wird das Fenster [IOU Split] nicht angezeigt.

1 Klicken Sie [Partition] → [Split Configuration] → [IOU Split].
Das Fenster [IOU Split] wird angezeigt.

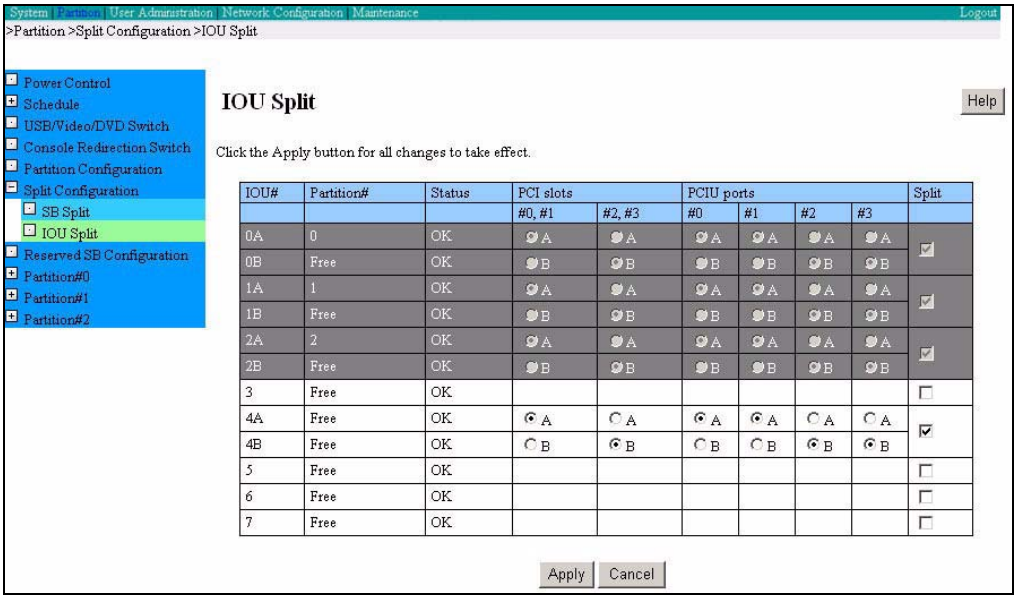


Abbildung 2.25 Fenster [IOU Split] (PRIMEQUEST 580A/540A*/580/540)

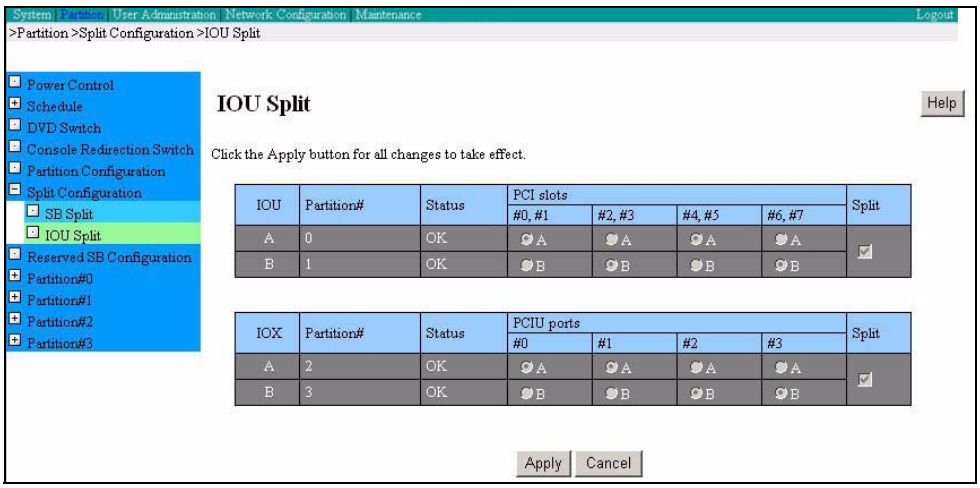


Abbildung 2.26 Fenster [IOU Split] (PRIMEQUEST 520A*/520)

*: wird von Fujitsu Technology Solutions nicht unterstützt

Tabelle 2.22 Feldnamen und mögliche Eingaben im Fenster [IOU Split]

Feld	Beschreibung
IOU#	Anzeige der IOU-Identifikationsnummer (ggf. zwei). Falls die IO Unit bereits geteilt ist, werden xA und xB angezeigt.
IOX (nur bei PRIMEQUEST 520A*/520)	Anzeige der IOX-Identifikationsnummer (ggf. zwei). Falls die IOX bereits geteilt ist, werden xA und xB angezeigt.
Partition#	Anzeige der Partition-Nummer oder „Free“ (die IO Unit oder IOX ist dann frei).
Status	Anzeige des IO Unit- oder IOX-Status.
PCI slots	PCI-Slot-Zuordnung zu den geteilten IO Units A und B.
PCIU ports	PCIU-Port-Zuordnung zu den geteilten IO Units oder IOXs A und B.
Split	Kontrollkästchen zum Teilen/Wiederverbinden der IO Unit oder IOX.

*: wird von Fujitsu Technology Solutions nicht unterstützt

- IO Unit oder IOX teilen:
  1. Aktivieren Sie das Kontrollkästchen [Split] der IO Unit oder IOX, die geteilt werden soll.
  2. Ordnen Sie mit den Optionsumschaltern [PCI slots] und [PCIU ports] den Teil-IO Units PCI-Slots und PCIU-Ports zu.
  3. Klicken Sie auf [Apply].
     Die IO Unit oder IOX wird geteilt, und im Fenster wird für die beiden Teile xA und xB angezeigt.
- IO Unit oder IOX wieder verbinden:
  1. Deaktivieren Sie das Kontrollkästchen [Split] der IO Unit oder IOX, deren beide Teile wieder verbunden werden sollen, und klicken Sie auf [Apply].
     Die Teile der IO Unit oder IOX werden wieder verbunden und als eine IO Unit oder IOX im Fenster angezeigt.

2.5.4 Partition konfigurieren

Dieser Abschnitt beschreibt, wie Systemboards, IO Units und IOXs hinzugefügt und entfernt
werden.

- Systemboards, IO Units und IOXs hinzufügen (→ 2.5.4.1)
- Systemboards, IO Units und IOXs entfernen (→ 2.5.4.2)

2.5.4.1 Systemboards, IO Units und IOXs hinzufügen

Sie können einer Partition ein Systemboard, eine IO Unit oder eine IOX hinzufügen.

Hinweise:

- Der Extended Mirror Mode kann nicht in Partitionen aktiviert werden, die Systemboards, IO Units oder IOXs enthalten, die mit XPAR geteilt wurden. Das Teilen von Systemboards, IO Units oder IOXs kann in Partitionen, in den der Extended Mirror Mode aktiviert ist, nicht durchgeführt werden.
- Ein Systemboard, das mit XPAR geteilt wurde, kann nicht als Systemboard für eine Partition reserviert werden, in der der Extended Mirror Mode aktiviert wurde.
  Der Extended Mirror Mode kann in Partitionen nicht aktiviert werden, für die geteilte Systemboards reserviert wurden.
- XPAR wird ausschließlich von der Modellreihe PRIMEQUEST 500A*/500 unterstützt, und die Beschaffung und Installation der XPAR-Option ist Voraussetzung für die Anwendung von XPAR.

Anm.: Ein Systemboard, eine IO Unit oder eine IOX können einer Partition bei laufendem Betriebssystem hinzugefügt werden. In diesem Falle muss die Partition neu gestartet werden, damit die neue Konfiguration in Kraft tritt.

Vorgehensweise

1 Wählen Sie [Partition] → [Partition Configuration].
Das Fenster [Partition Configuration] wird angezeigt.

*: wird von Fujitsu Technology Solutions nicht unterstützt

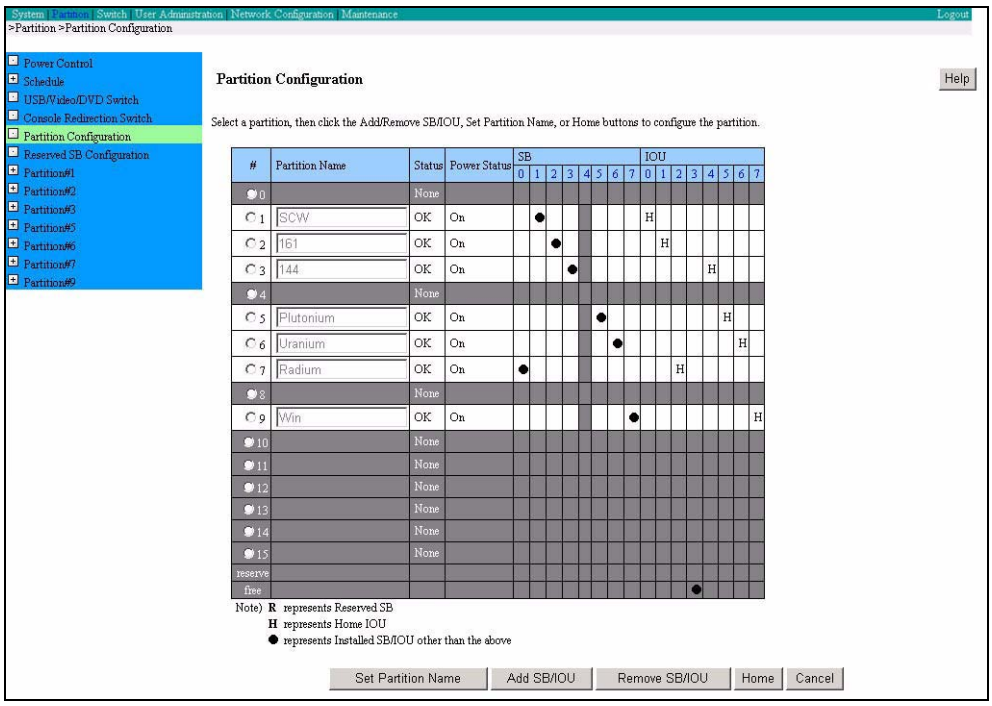


Abbildung 2.27 Das Fenster [Partition Configuration] (PRIMEQUEST 580A*/540A/580/540/480/440)

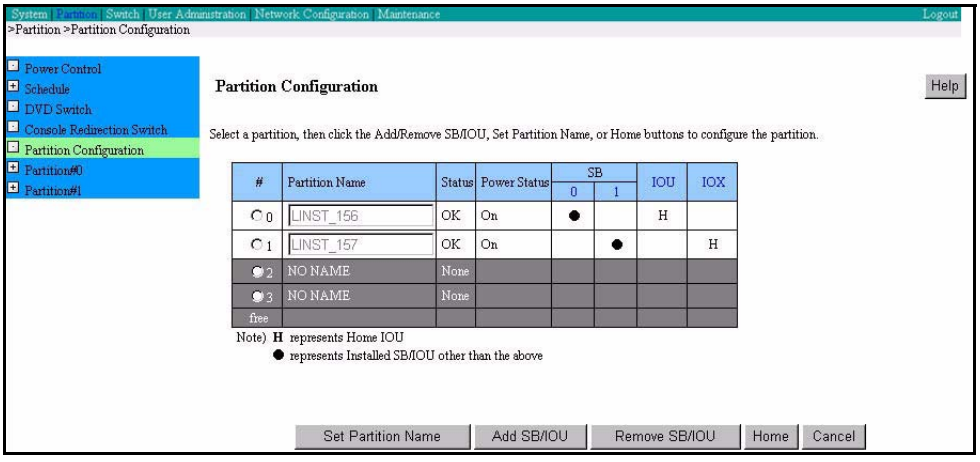

System | Partition | Switch | User Administration | Network Configuration | Maintenance
Logout
>Partition >Partition Configuration
Power Control
Schedule
DVD Switch
Console Redirection Switch
Partition Configuration
Partition#0
Partition#1
Partition Configuration
Help
Select a partition, then click the Add/Remove SB/IOU, Set Partition Name, or Home buttons to configure the partition.
| Partition Name | Status | Power Status | SB 0 1 | IOU | IOX
0 LINST_156 OK On H
1 LINST_157 OK On H
2 NO NAME None
3 NO NAME None
free
Note) H represents Home IOU
● represents Installed SB/IOU other than the above
Set Partition Name
Add SB/IOU
Remove SB/IOU
Home
Cancel

Abbildung 2.28 Das Fenster [Partition Configuration] (PRIMEQUEST 520A*/520/420)

*: wird von Fujitsu Technology Solutions nicht unterstützt

Tabelle 2.23 Feldnamen und mögliche Eingaben im Fenster [Partition Configuration]

Feldname	Beschreibung
#	Zeigt die ID-Nummer der Partition an. Bei einer PRIMEQUEST 580A/540A*/580/540/480/440, reichen die Nummern von 0 bis 15, bei einer PRIMEQUEST 520A*/520/420 von 0 bis 3.
Partition Name	Der einer Partition zugewiesene Name. Maximale Länge des Partitionsnamens: 16 Zeichen. Folgende Zeichen können verwendet werden: 0-9, a-z, A-Z, " " (en-size space), #, - (hyphen), _ (underscore) Anm.: Verwenden Sie zur leichteren Erkennung den Hostnamen, den Sie auch für das Betreibssystem verwendet haben.
Status	Zeigt den Status der Partition an. • OK: Normal • Degraded: Ein Komponentenfehler ist aufgetreten. (Die ausgefallene Komponente kann abgekoppelt werden, um mit dem Betrieb fortzufahren.) • Failed: Die Partition ist ausgefallen. • None: Keine Konfiguration vorhanden. Es sind keine Systemboards und IO Units zugewiesen.
Power Status	Einschaltstatus der Partition. • On: In Betrieb • Standby: Im Standby-Modus
SB	Das Symbol ● zeigt an, zu welcher Partition das Systemboard gehört. Ist das Systemboard in zwei Einheiten geteilt, erfolgt die Anzeige zweispaltig. Wenn kein Systemboard installiert ist, ist die entsprechende Spalte ausgegraut.
IOU	Das Symbol ● zeigt an, zu welcher Partition die IO Unit gehört. Ist die IO Unit in zwei Einheiten geteilt, erfolgt die Anzeige zweispaltig. Ein „H“ bedeutet, dass es sich um die Home IO Unit handelt. Wenn keine IO Unit installiert ist, ist die entsprechende Spalte ausgegraut.
IOX (nur PRIMEQUEST 520A*/ 520/420)	Das Symbol ● zeigt an, zu welcher Partition die IOX gehört. Ist die IOX in zwei Einheiten geteilt, erfolgt die Anzeige zweispaltig. Wenn keine IOX installiert ist, ist die entsprechende Spalte ausgegraut.

*: wird von Fujitsu Technology Solutions nicht unterstützt

2 Aktivieren Sie das Optionsfeld vor der Nummer der Partition, in der Sie ein Systemboard, eine IO Unit oder ein IOX hinzufügen wollen.

3 Klicken Sie dann auf die Schaltfläche [Add SB/IOU].
Das Fenster [Add SB/IOU to Partition] mit einer Liste der verfügbaren Systemboards, IO Units und IOXs erscheint.

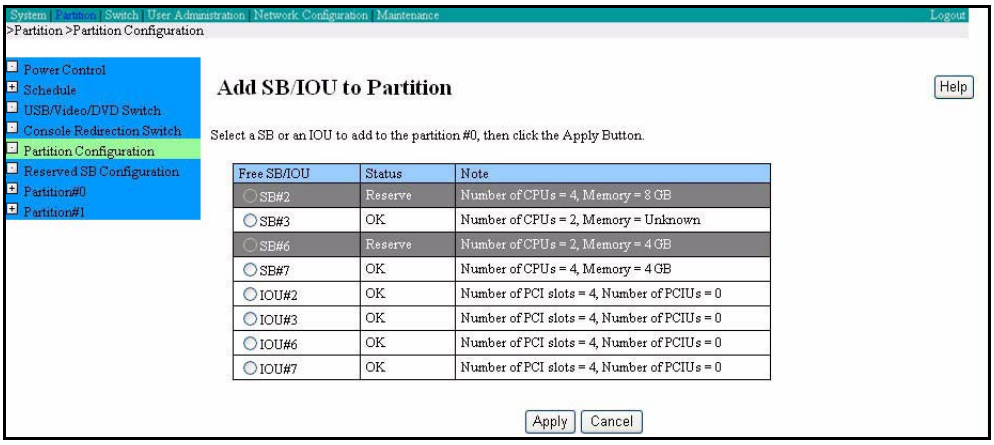


Abbildung 2.29 Das Fenster [Add SB/IOU to Partition]

Tabelle 2.24 Feldnamen und mögliche Eingaben im Fenster [Add SB/IOU to Partition]

Feldname	Beschreibung
Free SB/IOU	Zeigt freie Systemboards (d.h. Systemboards, die keiner Partition zugewiesen sind), IO Units und IOXs an.
Status	Zeigt den Status freier Systemboards, IO Units und IOXs an.
Note	(Bei Systemboards) • [Number of CPUs]: Gibt die Anzahl der auf dem Systemboard vorhandenen CPUs an. • [Memory]: Speicherkapazität des Systemboards. Hinweis: Wird ein Systemboard entfernt und wieder eingefügt, wird evtl. „unknown“ (unbekannte Speicherkapazität) ausgegeben.
Note	(Bei IO Unit oder IOX) • [Number of PCI slots]: Anzahl der PCI-Slots der IO Unit. • [Number of PCIUs]: Anzahl der mit der IO Unit verbundenen PCIs. • [Number of PEXU]: Anzahl der PCI Express Units, die mit der IO Unit verbunden sind.

4 Aktivieren Sie das Optionsfeld des Systemboards, der IO Unit oder der IOX, die einer Partition hinzugefügt werden soll.
Freie Systemboards, IO Units und IOXs können nur einzeln ausgewählt werden.

5 Klicken Sie auf [Apply], um die Eingaben zu übernehmen.
Es erscheint ein Bestätigungsfenster.

6 Klicken Sie auf [OK].
Das Systemboard, die IO Unit oder die IOX wird der Partition hinzugefügt.
Wiederholen Sie die Schritte 3 bis 6, bis Sie der Partition alle gewünschten Systemboards, IO Units oder IOxs hinzugefügt haben.

2.5.4.2 Systemboards, IO Units und IOXs entfernen

Dieser Abschnitt beschreibt, wie Sie aus einer Partition ein Systemboard, eine IO Unit oder eine IOX entfernen.

Anm.: Sie können ein Systemboard, eine IO Unit oder eine IOX nicht aus einer Partition entfernen, während deren Betriebssystem aktiv ist. Versetzen Sie die Partition hierfür zuerst in den Standby-Modus.

Vorgehensweise

1 Wählen Sie [Partition] → [Partition Configuration].
Das Fenster [Partition Configuration] wird angezeigt.

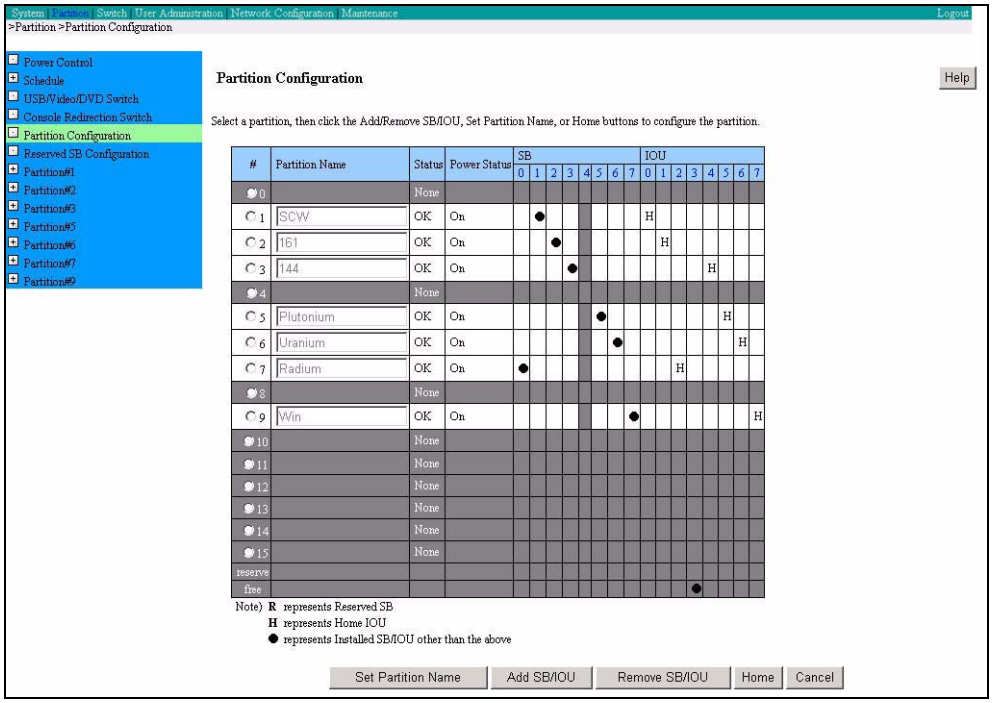


Abbildung 2.30 Das Fenster [Partition Configuration] (PRIMEQUEST 580A/540A*/580/540/480/440)

*: wird von Fujitsu Technology Solutions nicht unterstützt

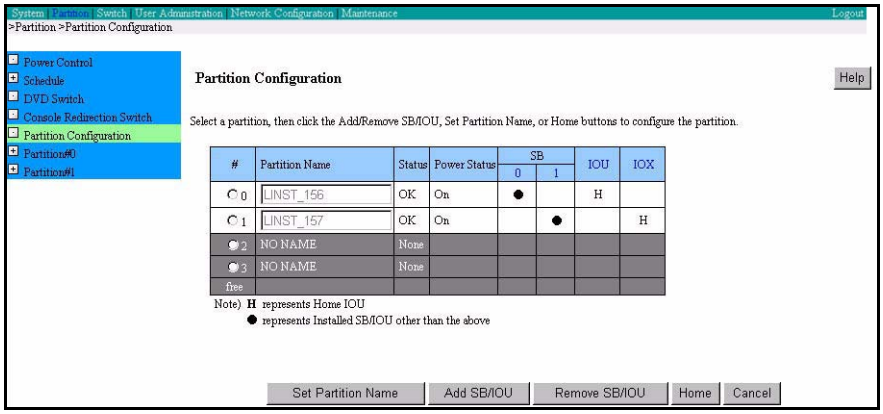

System | Partition | Switch | User Administration | Network Configuration | Maintenance
Logout
>Partition >Partition Configuration
Power Control
Schedule
DVD Switch
Console Redirection Switch
Partition Configuration
Partition#0
Partition#1
Partition Configuration
Help
Select a partition, then click the Add/Remove SB/IOU, Set Partition Name, or Home buttons to configure the partition.
| Partition Name | Status | Power Status | SB 0 | SB 1 | IOU | IOX
0 | LINST_156 | OK | On | ● | | H |
1 | LINST_157 | OK | On | | ● | | H
2 | NO NAME | None
3 | NO NAME | None
free
Note) H represents Home IOU
● represents Installed SB/IOU other than the above
Set Partition Name
Add SB/IOU
Remove SB/IOU
Home
Cancel

Abbildung 2.31 Das Fenster [Partition Configuration] (PRIMEQUEST 520A*/520/420)

2 Aktivieren Sie das Optionsfeld vor der Nummer der Partition, aus der Sie ein Systemboard, eine IO Unit oder eine IOX entfernen wollen.

3 Klicken Sie auf die Schaltfläche [Remove SB/IOU].
Das Fenster [Remove SB/IOU from Partition] mit einer Liste der der Partition zugewiesenen Systemboards, IO Units und IOXs erscheint.

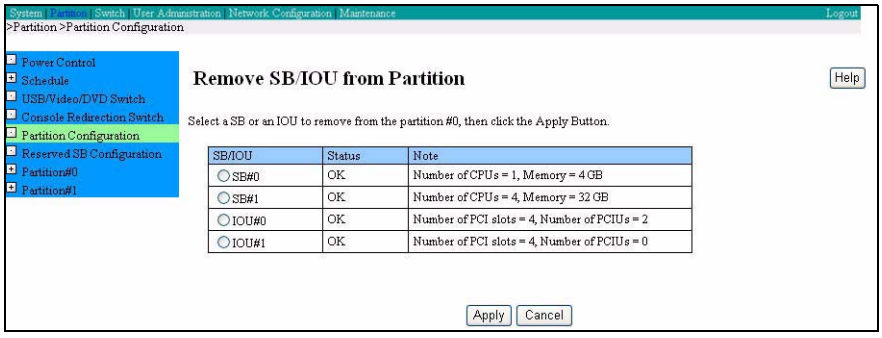

System | Partition | Switch | User Administration | Network Configuration | Maintenance
Logout
>Partition >Partition Configuration
Power Control
Schedule
USB/Video/DVD Switch
Console Redirection Switch
Partition Configuration
Reserved SB Configuration
Partition#0
Partition#1
Remove SB/IOU from Partition
Help
Select a SB or an IOU to remove from the partition #0, then click the Apply Button.
SB/IOU | Status | Note
SB#0 | OK | Number of CPUs = 1, Memory = 4 GB
SB#1 | OK | Number of CPUs = 4, Memory = 32 GB
IOU#0 | OK | Number of PCI slots = 4, Number of PCIUs = 2
IOU#1 | OK | Number of PCI slots = 4, Number of PCIUs = 0
Apply
Cancel

Abbildung 2.32 Das Fenster [Remove SB/IOU from Partition]

*: wird von Fujitsu Technology Solutions nicht unterstützt

Tabelle 2.25 Feldnamen und mögliche Eingaben im Fenster [Remove SB/IOU from Partition]

Feldname	Beschreibung
SB/IOU	Zeigt die Systemboards, IO Units und IOXs der Partition an.
Status	Zeigt deren jeweiligen Status an.
Note	(Bei Systemboards) • [Number of CPUs]: Gibt die Anzahl der auf dem Systemboard vorhandenen CPUs an. • [Memory]: Speicherkapazität des Systemboards. Hinweis: Wird ein Systemboard entfernt und wieder eingefügt, wird evtl. „unknown“ (unbekannte Speicherkapazität) ausgegeben.
Note	(Bei IO Unit oder IOX) • [Number of PCI slots]: Anzahl der PCI-Slots der IO Unit. • [Number of PCIUs]: Anzahl der mit der IO Unit verbundenen PCIs. • [Number of PEXU]: Anzahl der PCI Express Units, die mit der IO Unit verbunden sind.

4 Aktivieren Sie das Optionsfeld des Systemboards, der IO Unit oder der IOX, die aus der Partition entfernt werden soll. Es kann immer nur ein Systemboard, eine IO Unit oder eine IOX ausgewählt werden.

5 Klicken Sie auf [Apply], um die Eingaben zu übernehmen.
Es erscheint ein Bestätigungsfenster.

6 Klicken Sie auf die Schaltfläche [OK].
Das Systemboard, die IO Unit oder die IOX wird aus der Partition entfernt und wird frei.

2.5.5 Home IO Unit festlegen

Mit dieser Funktion definieren Sie eine der in der Partition eingehängten IO Units und IOXs als die Home IO Unit.

Vorgehensweise

1 Nachdem Sie zu einer Partition alle gewünschten Systemboards, IO Units und IOXs hinzugefügt haben, wählen Sie [Partition] → [Partition Configuration].
Das Fenster [Partition Configuration] wird angezeigt.

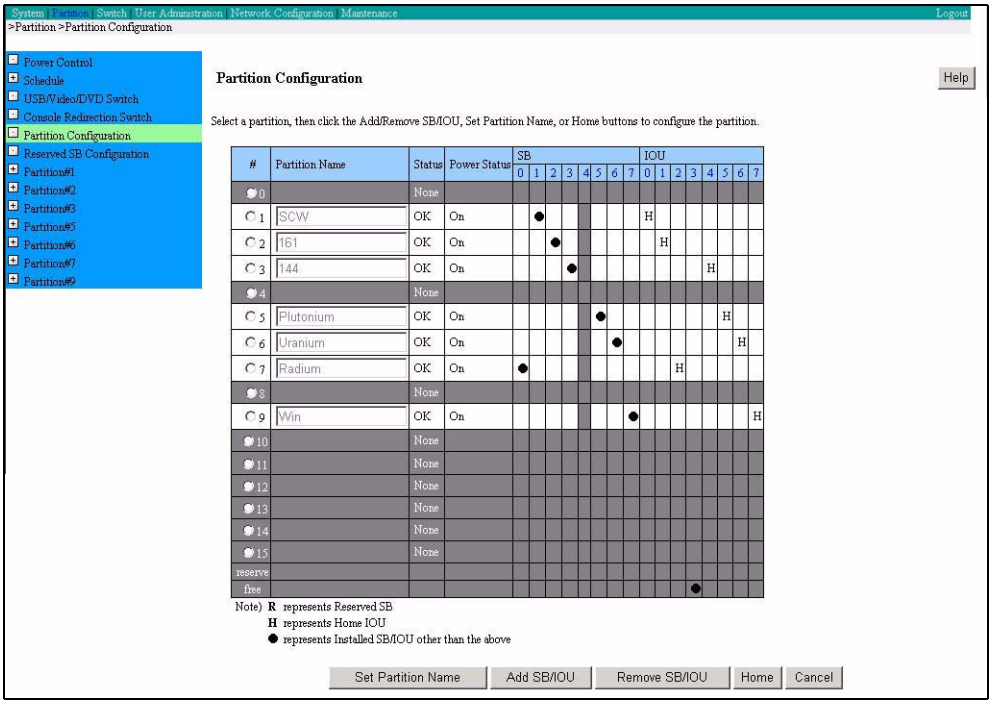


Abbildung 2.33 Das Fenster [Partition Configuration] (PRIMEQUEST 580A/540A*/580/540/480/440)

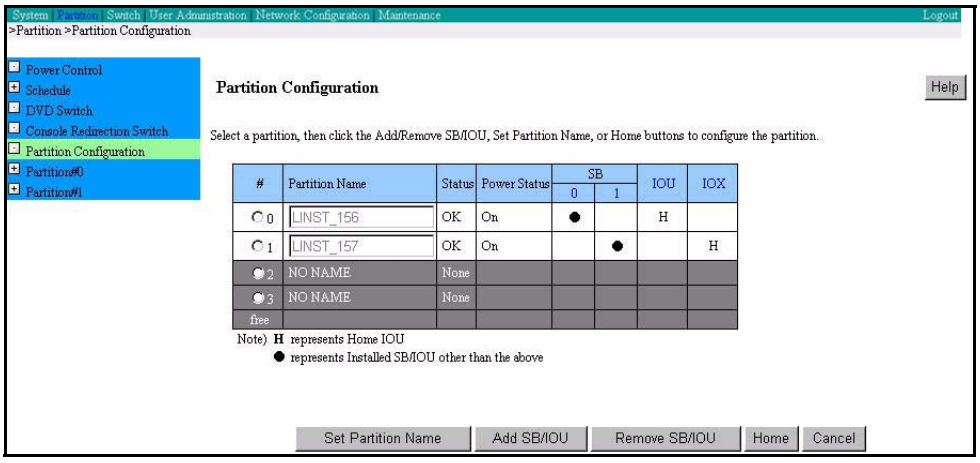


Abbildung 2.34 Das Fenster [Partition Configuration] (PRIMEQUEST 520A*/520/420)

2 Wählen Sie die Partition aus, der Sie eine Home IO Unit hinzufügen wollen und klicken Sie dann auf die Schaltfläche [Home].
Das Fenster [Partition Home] wird angezeigt.

*: wird von Fujitsu Technology Solutions nicht unterstützt

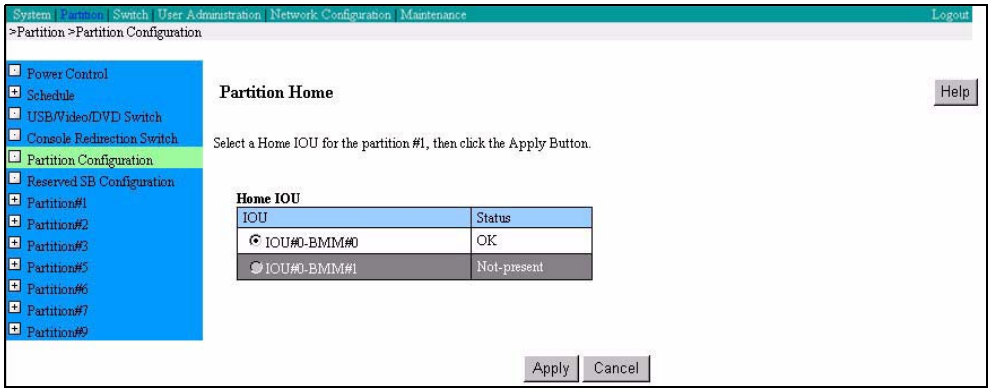


Abbildung 2.35 Das Fenster [Partition Home]

Tabelle 2.26 Feldnamen und mögliche Eingaben im Fenster [Partition Home]

Feldname	Beschreibung
<Home IOU>	
IOU	Zeigt die IO Units und IOXs an, die BMMs enthalten und die einer Partition zugeweisen sind.
Status	Zeigt den Status des Ziel-BMMs an.

3 Aktivieren Sie das Optionsfeld der IO Unit oder IOX, die als Home dienen soll.
Hinweis: Wählen Sie als Home-Systemboard stets das Systemboard mit der niedrigsten Nummer.

4 Klicken Sie auf [Apply], um die Eingaben zu übernehmen.
Die betreffende IO Unit oder IOX wird zur Home-Einheit der Partition. In der entsprechenden Spalte des Fensters [Partition Configuration] erscheint ein „H“.

2.5.6 Systemboard reservieren

Ein reserviertes Systemboard ist entsprechend vorbereitet, um das Systemboard einer Partition im Fehlerfall zu ersetzten. Der Benutzer kann Systemboards für bestimmte Partitionen reservieren. Es kann auch eine der beiden Einheiten eines geteilten Systembords für eine Partition reserviert werden

Hinweise:

- Wenn ein Systemboardfehler zu einem Neustart der Partition führt, wir auf das in der Partition als reserviert eingetragenen Systemboard umgeschaltet.
  Wenn in einer (dupliziert-)redundanten Konfiguration im Extended Mirror Mode eine der Komponenten (wie z. B. Hauptspeicher) ausfällt und die andere Komponente ohne Unterbrechung weiterarbeitet, wird nicht auf das reservierte Systemboard umgeschaltet.
- Ein Systemboard, das mit XPAR geteilt wurde, kann nicht als Systemboard für eine Partition reserviert werden, in der der Extended Mirror Mode aktiviert wurde.
  Der Extended Mirror Mode kann in Partitionen nicht aktiviert werden, für die geteilte Systemboards reserviert wurden.
- Das Systemboard, das für eine Partition reserviert wird, sollte den gleichen Speicher und die gleiche Anzahl CPUs haben wie die in einer Partition konfigurierten Systemboards. Wenn sich die Anzahl CPUs beim Wechsel zu einem reservierten Systemboard erhöht, sind andernfalls zusätzliche Lizenzen erforderlich.
- Das Systemboard, das für eine Partition reserviert wird, muss den gleichen CPU-Typ haben wie die in einer Partition konfigurierten Systemboards. Ein Systemboard, das einen anderen CPU-Typ enthält, kann nicht als Reserve-Systemboard definiert werden.
- Ein Systemboard, das mit 32 GB (8-GB DIMM x 4) Hauptspeicher bestückt ist, kann nicht zusammen in derselben Partition mit einem Systemboard anderer Hauptspeicherbestückung betrieben werden.
- Ein Systemboard, das mit 16 GB (4-GB DIMM x 4) Hauptspeicher bestückt ist, kann nicht zusammen in derselben Partition mit einem Systemboard anderer Hauptspeicherbestückung betrieben werden.
  Deshalb kann ein Systemboard, das mit 16 GB (4-GB DIMM x 4) Hauptspeicher bestückt ist, nicht für eine Partition mit anderer Hauptspeicherbestückung eingesetzt werden.
- Wenn in einer Partition Windows Server 2003 installiert ist und nach einer Umschaltung auf ein reserviertes Systemboard die Partition zum ersten Mal startet, verlangt die Partition die Bestätigung zu ihrem Neustart. Starten Sie die Partition wie verlangt so schnell wie möglich.

- Berücksichtigen Sie bei der Abschätzung der Zeit, die eine Partition mit Windows Server 2003 gestoppt ist, die für den Neustart benötigte Zeitspanne. Die Gesamtzeit bis zur Wiederaufnahme des Betriebs setzt sich zusammen aus dem Zeitbedarf für den Neustart und die Zeit für den Betriebssystemstart nach dem Umschalten zum reservierten Systemboard.

Vorgehensweise

1 Wählen Sie [Partition] → [Reserved Configuration].
Das Fenster [Reserved Configuration] wird angezeigt.
Die Kontrollkästchen erscheinen in der Systemboard-Spalte mit den freien bzw. reservierten Systemboards.
Anmerkung: Bei der PRIMEQUEST 500-Reihe hängt der Inhalt des [Reserved SB Configuration]-Fensters von der MMB-Firmwareversion ab. Handelt es sich um Version 3.24 oder später, werden die Fenster in Abbildung 2.36 oder Abbildung 2.39 gezeigt. Handelt es sich um Version 3.23 oder früher, werden die Fenster in Abbildung 2.37 oder Abbildung 2.40 gezeigt. Die Firmwareversion lässt sich im Fenster [Firmware Information] ermitteln (klicken Sie hierzu [System] → [Firmware Information]).

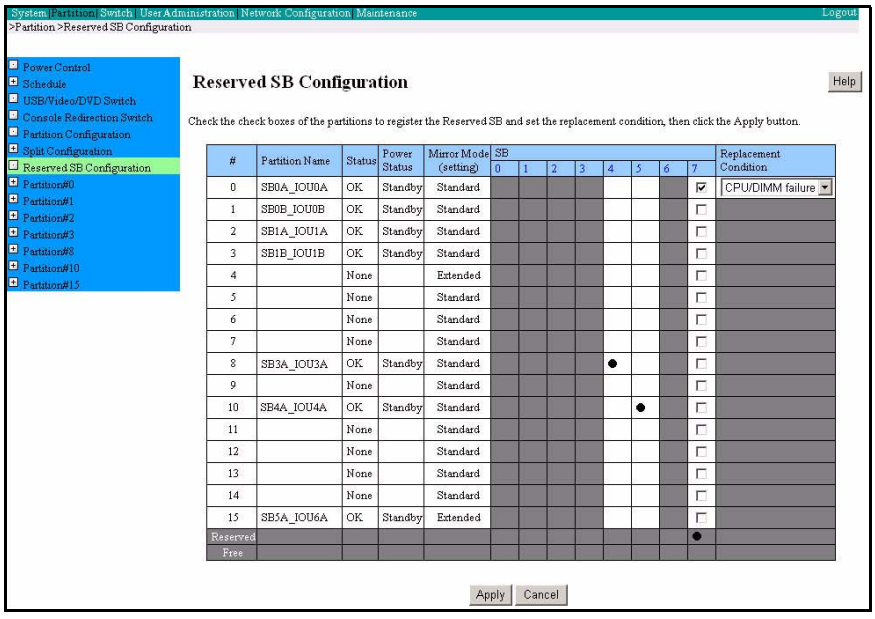

System Partition Switch User Administration Network Configuration Maintenance Logout
>Partition >Reserved SB Configuration
Power Control
Schedule
USB/Video/DVD Switch
Console Redirection Switch
Partition Configuration
Split Configuration
Reserved SB Configuration
Partition#0
Partition#1
Partition#2
Partition#3
Partition#8
Partition#10
Partition#15
Reserved SB Configuration
Help
Check the check boxes of the partitions to register the Reserved SB and set the replacement condition, then click the Apply button.
| Partition Name | Status | Power Status | Mirror Mode (setting) | SB 0 1 2 3 4 5 6 7 | Replacement Condition
0 | SB0A_IOU0A | OK | Standby | Standard | CPU/DIMM failure
1 | SB0B_IOU0B | OK | Standby | Standard
2 | SB1A_IOU1A | OK | Standby | Standard
3 | SB1B_IOU1B | OK | Standby | Standard
4 | None | Extended
5 | None | Standard
6 | None | Standard
7 | None | Standard
8 | SB3A_IOU3A | OK | Standby | Standard
9 | None | Standard
10 | SB4A_IOU4A | OK | Standby | Standard
11 | None | Standard
12 | None | Standard
13 | None | Standard
14 | None | Standard
15 | SB5A_IOU6A | OK | Standby | Extended
Reserved
Free
Apply
Cancel

Abbildung 2.36 Das Fenster [Reserved SB Configuration] (PRIMEQUEST 580A/540A* und PRIMEQUEST 580/540: Anzeige bei MMB-Firmwareversion 3.24 oder später)

*: wird von Fujitsu Technology Solutions nicht unterstützt

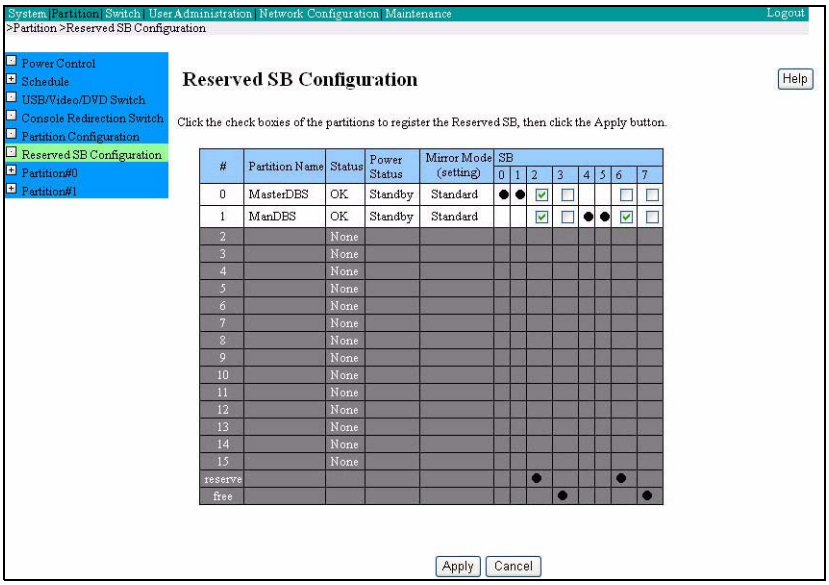

System | Partition | Switch | User Administration | Network Configuration | Maintenance
Logout
>Partition >Reserved SB Configuration
Power Control
Schedule
USB/Video/DVD Switch
Console Redirection Switch
Partition Configuration
Reserved SB Configuration
Partition#0
Partition#1
Reserved SB Configuration
Help
Click the check boxies of the partitions to register the Reserved SB, then click the Apply button.
| Partition Name | Status | Power Status | Mirror Mode (setting) | SB 0 1 2 3 4 5 6 7
0 | MasterDBS | OK | Standby | Standard
1 | ManDBS | OK | Standby | Standard
2 | None
3 | None
4 | None
5 | None
6 | None
7 | None
8 | None
9 | None
10 | None
11 | None
12 | None
13 | None
14 | None
15 | None
reserve
free
Apply
Cancel

Abbildung 2.37 Das Fenster [Reserved SB Configuration] (PRIMEQUEST 580/540: Anzeige bei MMB-Firmwareversion 3.23 oder früher.)

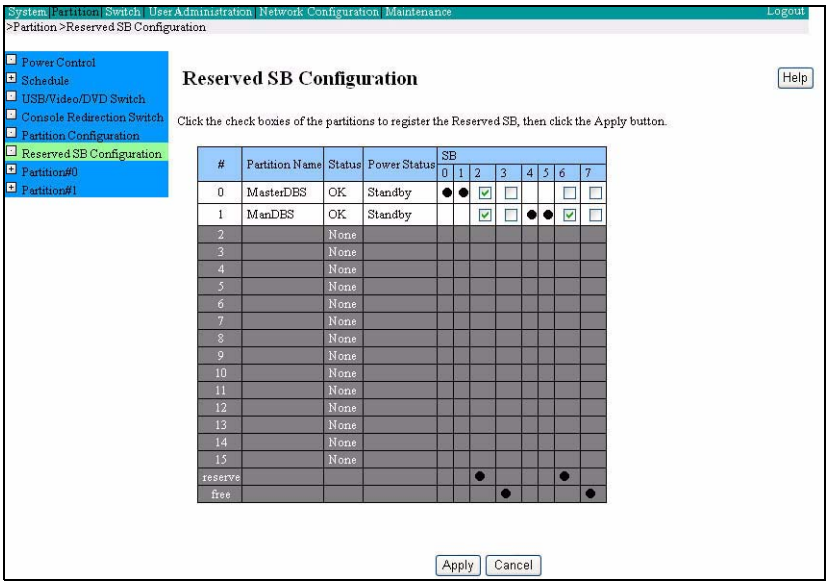


Abbildung 2.38 Das Fenster [Reserved SB Configuration] (PRIMEQUEST 480/440)

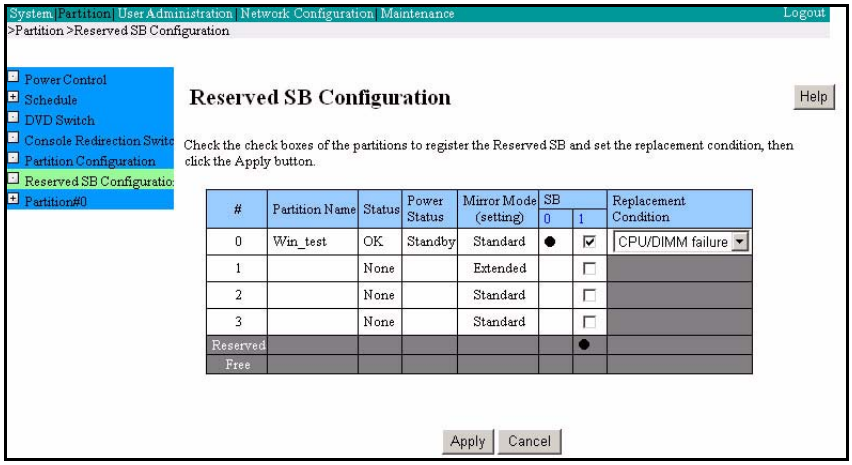

System Partition User Administration Network Configuration Maintenance Logout
>Partition >Reserved SB Configuration
Power Control
Schedule
DVD Switch
Console Redirection Switc
Partition Configuration
Reserved SB Configuratio
Partition#0
Reserved SB Configuration
Help
Check the check boxes of the partitions to register the Reserved SB and set the replacement condition, then click the Apply button.
Partition Name Status Power Status Mirror Mode (setting) SB 0 SB 1 Replacement Condition
0 Win_test OK Standby Standard CPU/DIMM failure
1 None Extended
2 None Standard
3 None Standard
Reserved
Free
Apply Cancel

Abbildung 2.39 Das Fenster [Reserved SB Configuration] (PRIMEQUEST 520A* und PRIMEQUEST 520: Anzeige bei MMB-Firmwareversion 3.24 oder später.)

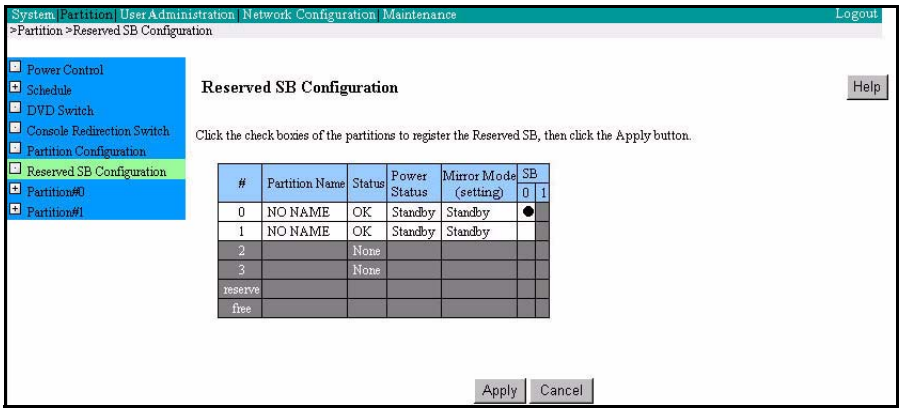


Abbildung 2.40 Das Fenster [Reserved SB Configuration] (PRIMEQUEST 520: Anzeige bei MMB-Firmwareversion 3.23 oder früher)

*: wird von Fujitsu Technology Solutions nicht unterstützt

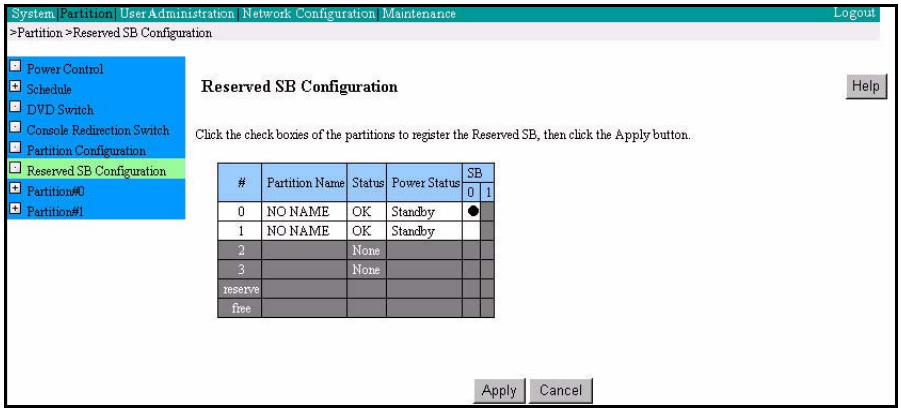


Abbildung 2.41 Das Fenster [Reserved SB Configuration] (PRIMEQUEST 420)

2 Klicken Sie das Kontrollkästchen der Ziel-Partition in einer Spalte an, die ein Systemboard enthält, das bislang noch keiner Partition zugewiesen wurde (freies oder reserviertes Systemboard).

3 Mit [Replacement Condition] werden die Zeitbedingungen für das Umschalten auf ein reserviertes Systemboard eingestellt

[Beginn der Korrektur gemäß Handbuch-Errata 2008/12/18]:

~~(PRIMEQUEST 580A/540A*/520A* oder PRIMEQUEST 500 mit MMB-Firmwareversion 3.24 oder später)~~

Anm.: Dieser Wert kann für die Systeme PRIMEQUEST 580A/540A/520A oder PRIMEQUEST 500 eingestellt werden, auf denen die MMB-Firmware mit Version 3.24 oder jünger läuft.

- SB-Fehlker: Wenn ein SB in der Partition ausfällt, wird es durch das hierfür vorgesehene Reserved SB ersetzt.
- CPU/DIMM-Fehler: Wenn eine CPU oder ein DIMM auf einem SB in der Partition ausfällt, wird das SB durch das hierfür vorgesehene Reserved SB ersetzt

Standardwert ist [CPU/DIMM-Fehler].

[Ende der Korrektur gemäß Handbuch-Errata 2008/12/18]

4 Klicken Sie dann auf [Apply], um die Eingabe zu bestätigen.

Hinweis: Um ein reserviertes Systemboard wieder freizugeben, deaktivieren Sie dessen Kontrollkästchen im Fenster [Reserved SB Configuration].

*: wird von Fujitsu Technology Solutions nicht unterstützt

2.5.7 Partitionsnamen festlegen

Mit dieser Funktion können Sie die Partitionsnamen festlegen. Dazu sind Systemverwalterrechte erforderlich.

Vorgehensweise

1 Wählen Sie [Partition] → [Partition Configuration].
Das Fenster [Partition Configuration] wird angezeigt.

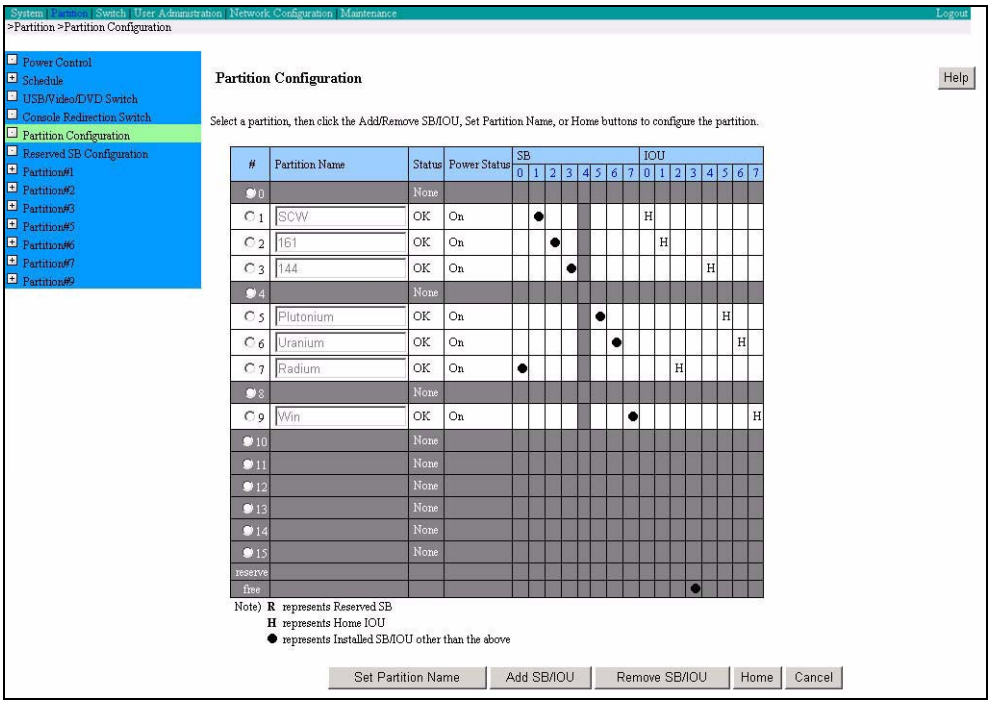


Abbildung 2.42 Das Fenster [Partition Configuration] (PRIMEQUEST 580A/540A*/580/540/480/440)

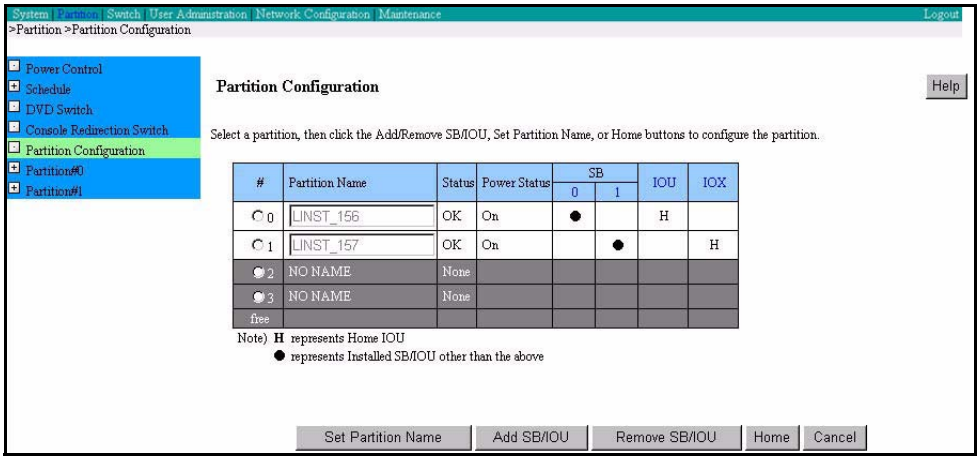

System | Partition | Switch | User Administration | Network Configuration | Maintenance
Logout
>Partition >Partition Configuration
Power Control
Schedule
DVD Switch
Console Redirection Switch
Partition Configuration
Partition#0
Partition#1
Partition Configuration
Help
Select a partition, then click the Add/Remove SB/IOU, Set Partition Name, or Home buttons to configure the partition.
| Partition Name | Status | Power Status | SB 0 1 | IOU | IOX
0 LINST_156 OK On ● H
1 LINST_157 OK On ● H
2 NO NAME None
3 NO NAME None
free
Note) H represents Home IOU
● represents Installed SB/IOU other than the above
Set Partition Name
Add SB/IOU
Remove SB/IOU
Home
Cancel

Abbildung 2.43 Das Fenster [Partition Configuration] (PRIMEQUEST 520A*/520/420)

*: wird von Fujitsu Technology Solutions nicht unterstützt

2 Wählen Sie die Partition aus, der Sie einen Partitionsnamen zuweisen wollen und geben Sie den Namen im Feld [Partition Name] ein.
Anm.:

- Sie können maximal 16 Zeichen verwenden. Folgende Zeichen können verwendet werden:
  0-9, a-z, A-Z, " " (en-size space), #, - (hyphen), _ (underscore)
- Benutzen Sie denselben Namen wie im Betriebssystem, damit er leichter erkennbar ist.

3 Klicken Sie auf die Schaltfläche [Set Partition Name].
Der Name der Partition ist somit festgelegt.

2.5.8 Verschiedene Modes einstellen

Mit dieser Funktion stellen Sie den PCI-Adressierungsmodus (nur PRIMEQUEST 580A/540A*/580/540/480/440), den System Mirror Mode und den Hyper Threading Mode (nur für Modellreihe PRIMEQUEST 500A/500) ein.

Beachten Sie die folgenden Hinweise zu XPAR.

Hinweise:

- Der Extended Mirror Mode kann nicht in Partitionen aktiviert werden, die Systemboards, IO Units oder IOXs enthalten, die mit XPAR geteilt wurden. Teile eines geteilten Systemboard, einer geteilten IO Unit oder einer geteilten IOX können keiner Partition zugeordnet werden, in der der Extended Mirror Mode aktiviert.
- Ein Systemboard, das mit XPAR geteilt wurde, kann nicht als Systemboard für eine Partition reserviert werden, in der der Extended Mirror Mode aktiviert wurde. Der Extended Mirror Mode kann in Partitionen nicht aktiviert werden, für die geteilte Systemboards reserviert wurden.
- XPAR wird ausschließlich von der Modellreihe PRIMEQUEST 500A/500 unterstützt, und die Beschaffung und Installation der XPAR-Option ist Voraussetzung für die Anwendung von XPAR.

Vorgehensweise

1 Wählen Sie [Partition] → [Partition#x] → [Mode].
Das Fenster [Mode] wird angezeigt.

*: wird von Fujitsu Technology Solutions nicht unterstützt

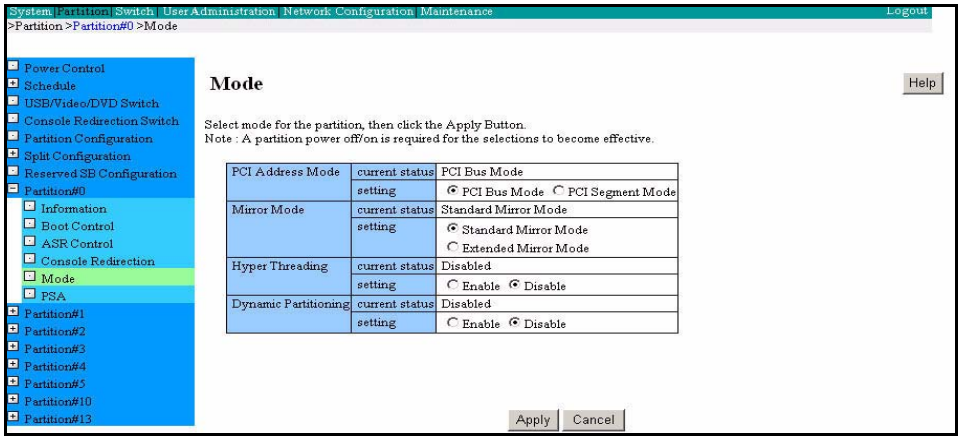


Abbildung 2.44 Das Fenster [Mode] (PRIMEQUEST 580A/540A*)

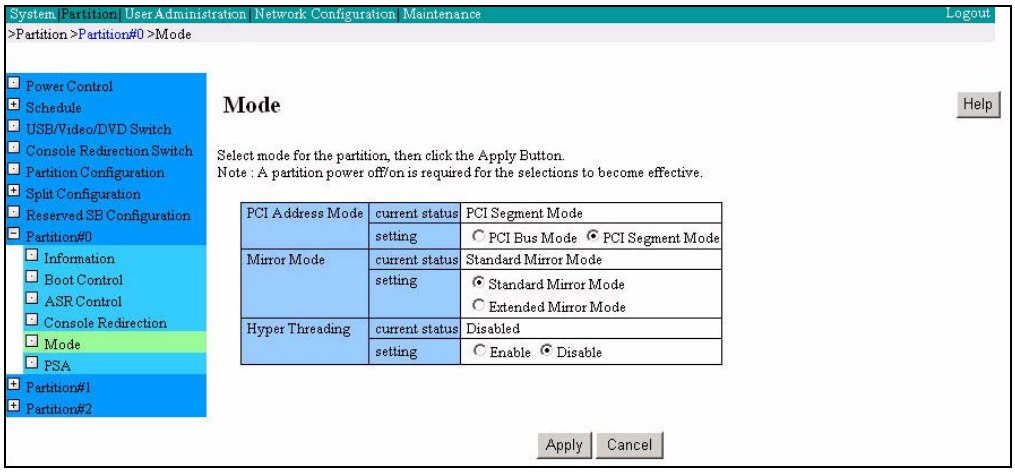


Abbildung 2.45 Das Fenster [Mode] (PRIMEQUEST 580/540)

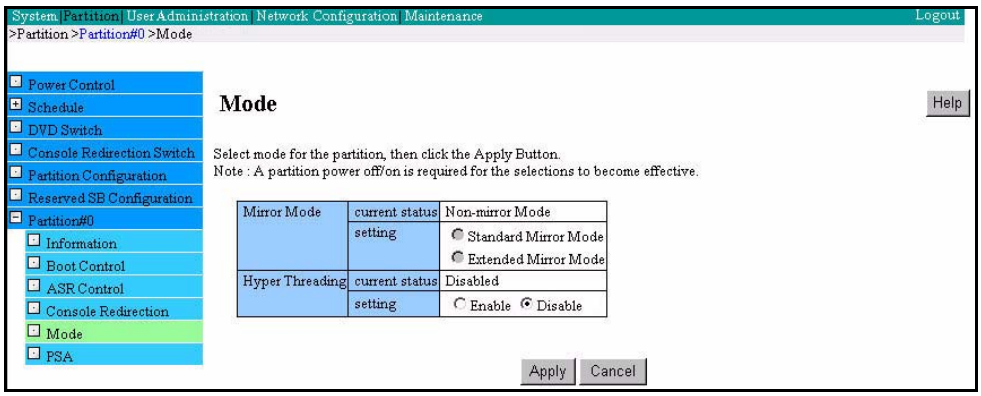


Abbildung 2.46 Das Fenster [Mode] (PRIMEQUEST 520A*/520)

*: wird von Fujitsu Technology Solutions nicht unterstützt

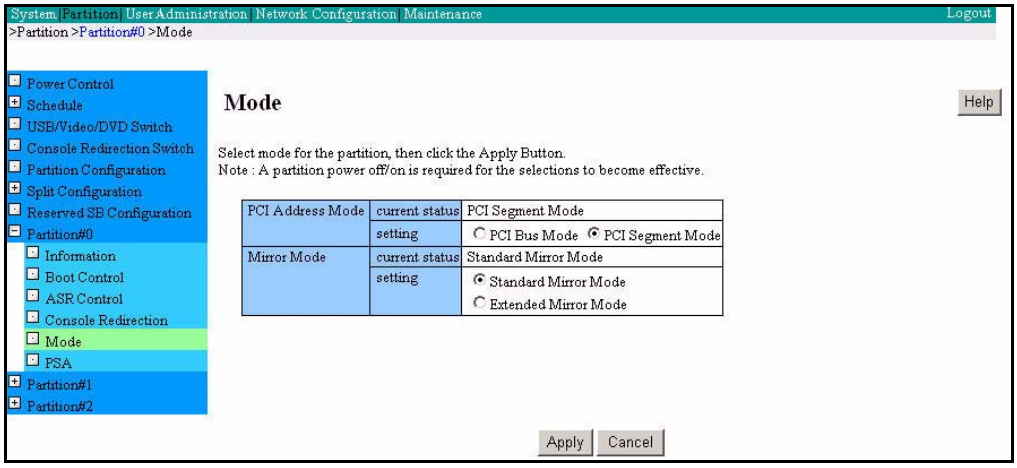


Abbildung 2.47 Das Fenster [Mode] (PRIMEQUEST 480/440)

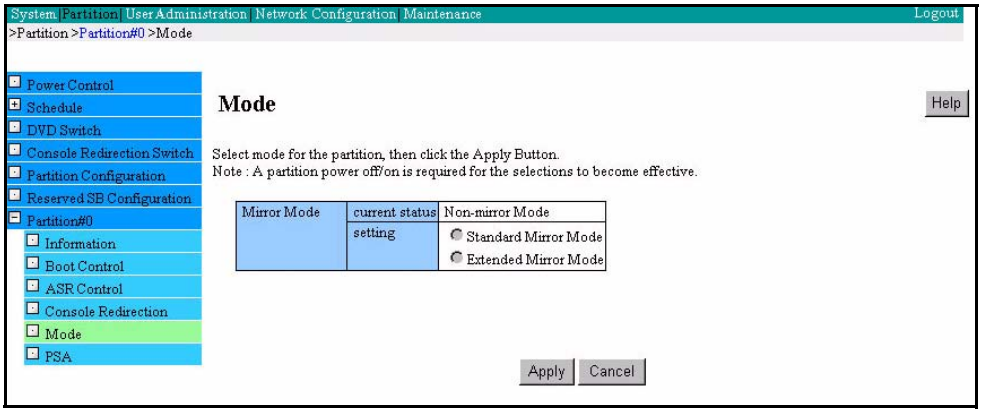


Abbildung 2.48 Das Fenster [Mode] (PRIMEQUEST 420)

2 Stellen Sie verschiedene Modes ein.

Anmerkung: Einzelheiten zu den Dynamic Partitioning-Einstellungen finden Sie im Handbuch *PRIMEQUEST 580A/540A DP (Dynamic Partitioning) Manual* (U41799-J-Z816-x-76/C122-E085EN).

Tabelle 2.27 Feldnamen und mögliche Eingaben im Fenster [Mode]

Feldname	Beschreibung
PCI Address Mode (current status) (nur PRIMEQUEST 580A/540A*/580/540/ 480/440)	Zeigt den aktuellen PCI-Adressierungsmodus der Partition an. • [PCI Bus Mode]: Alle PCI-Slots der Partition werden unter der Segmentnummer 0 definiert. • [PCI Segment Mode]: Die PCI-Slots der Partition werden für jede IO Unit Segment für Segment definiert. Wenn [PCI Segment Mode] verwendet wird, erscheint ein PCI-Gerät unter IOU#0 unter dem Segment 0 und ein PCI-Gerät unter der IOU#1 unter dem Segment 1.
PCI Address Mode (setting) (nur PRIMEQUEST 580A/540A*/580/540/ 480/440)	Legt den PCI-Adressierungsmodus der Partition fest. Der Modus tritt nach einem Neustart der Partition in Kraft. Hinweis: • Wählen Sie [PCI Bus Mode] für die Partition, in der als Betriebssystem Windows Server 2003 verwendet wird. • Wählen Sie [PCI Segment Mode] für die Partition, in der als Betriebssystem Linux verwendet wird. • Falls Linux installiert wurde, muss [PCI Bus Mode] eingestellt werden. • Informationen zum Einstellen des PCI Address Mode für Partitionen, auf denen Windows Server 2008 läuft, finden Sie im Handbuch *PRIMEQUEST Windows Server 2008 User's Guide* (U41805-J-Z816-x-76/C122-E087EN).
Interleave Mode between SBs (nur PRIMEQUEST 480/ 440)	Anmerkung: Dieser Mode wird für Systeme PRIMEQUEST 480/440 angezeigt. Verwenden Sie diesen Mode jedoch nicht.
Mirror Mode (Current status)	Zeigt den aktuell eingestellten Modus an.
Mirror Mode (setting)	Legt den zu verwendenden Mirror Mode fest. Einzelheiten zum Mirror Mode finden Sie im *System Design Guide*. • Standard Mirror Mode • Extended Mirror Mode Hinweis:Wenn [Mirror Mode] im Fenster [System Setup] auf [Disable] gesetzt ist, erscheint die Option [Mirror Mode] hier ausgegraut. d.h. sie kann nicht ausgewählt werden. Voreinstellung: [Standard Mirror Mode].
Hyper Threading (current) (nur für Modellreihe PRIMEQUEST 500A/ 500)	Zeigt an, ob Hyper Threading aktiviert oder deaktiviert ist. • Enabled: Hyper Threading ist aktiviert. • Disabled: Hyper Threading ist deaktiviert.

Tabelle 2.27 Feldnamen und mögliche Eingaben im Fenster [Mode]

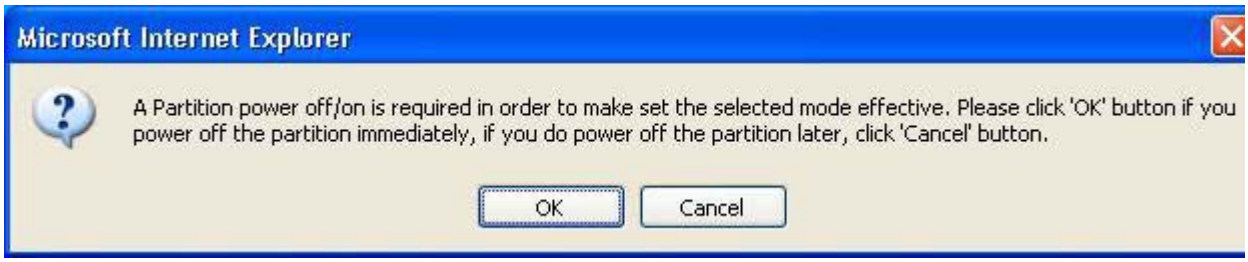
Feldname	Beschreibung
Hyper Threading (setting) (nur für Modellreihe PRIMEQUEST 500A/ 500)	Aktiviert oder deaktiviert Hyper Threading. • Enable: Aktiviert Hyper Threading. • Disable: Deaktiviert Hyper Threading. Standardeinstellung ist [Disable] (deaktiviert).
Dynamic Partitioning (current) (nur PRIMEQUEST 580A/540A*)	Zeigt an, ob Dynamic Partitioning aktiviert oder deaktiviert ist. Enabled: Dynamic Partitioning ist aktivier. Disabled: Dynamic Partitioning ist deaktiviert.
Dynamic Partitioning (setting) (nur PRIMEQUEST 580A/540A*)	Aktiviert oder deaktiviert Dynamic Partitioning. Enable: Aktiviert Dynamic Partitioning. Disable: Deaktiviert Dynamic Partitioning. Anmerkung: In allen im Folgenden aufgeführten Fällen wird Dynamic Partitioning nicht unterstützt. In diesen Fällen stellen Sie bitte [Disable] ein, weil die Funktion nicht garantiert werden kann; die Einstellung [Enable] führt möglicherweise zu einer nicht korrekten Installation. • Das System läuft unter RHEL mit einer Version kleiner als 5.1 (IPF). • Das System läuft unter Windows mit einer Version kleiner als Windows Server 2008. • Das System läuft unter SUSE. • Die Virtualisierungsfunktionen des Systems werden benutzt. Standardeinstellung ist [Disable] (Deaktiviere Dynamic Partitioning) Einzelheiten finden Sie im Handbuch *PRIMEQUEST 580A/ 540A Dynamic Partitioning (DP) Manual* (U41799-J-Z816-x-76/C122-E085EN).

*: wird von Fujitsu Technology Solutions nicht unterstützt

WICHTIG

- Änderungen werden erst nach einem Aus-/Einschalten der Partition wirksam.

3 Klicken Sie auf [Apply].
Ein Fenster zur Bestätigung wird angezeigt.


Microsoft Internet Explorer
A Partition power off/on is required in order to make set the selected mode effective. Please click 'OK' button if you power off the partition immediately, if you do power off the partition later, click 'Cancel' button.
OK
Cancel

2.5.9 Partition starten

In diesem Abschnitt wird beschrieben, wie Sie eine in Betrieb befindliche Partition starten.

Vorgehensweise

1 Wählen Sie [Partition] → [Power Control] aus.
Das Fenster [Power Control] wird angezeigt.

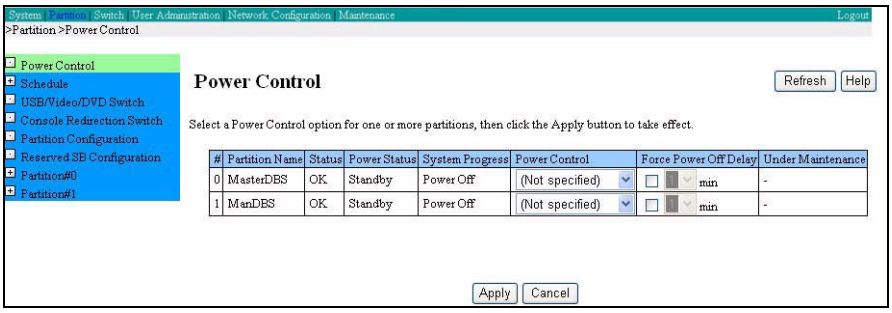

System | Partition | Switch | User Administration | Network Configuration | Maintenance
Logout
>Partition >Power Control
Power Control
Schedule
USB/Video/DVD Switch
Console Redirection Switch
Partition Configuration
Reserved SB Configuration
Partition#0
Partition#1
Power Control
Refresh
Help
Select a Power Control option for one or more partitions, then click the Apply button to take effect.
| Partition Name | Status | Power Status | System Progress | Power Control | Force Power Off Delay | Under Maintenance
0 | MasterDBS | OK | Standby | Power Off | (Not specified) | min | -
1 | ManDBS | OK | Standby | Power Off | (Not specified) | min | -
Apply
Cancel

Abbildung 2.49 Das Fenster [Power Control]

2 Wählen Sie im Fenster [Power Control] für die betreffende Partition die Option [Power on] aus und klicken Sie auf [Apply].

Tabelle 2.28 Feldnamen und mögliche Eingaben im Fenster [Power Control]

Feld	Beschreibung
Power Control	Wählen Sie die Power Control-Einstellung für die Partition aus. Der Option [Power On] wird für eine eingeschaltete Partition nicht angeboten. Umgekehrt werden die Optionen Power Off], [Power Cycle], [Reset], [INIT], und [Force Power Off] für ausgeschaltete Partitionen nicht angeboten. • Power On: Schaltet die Partition ein. • Power Off: Schaltet die Partition aus. • Power Cycle: Erzwingt das Aus- und wieder Einschalten der Partition. • Reset: Setzt die Partition zurück. • INIT: Erzeugt für die Partition ein INIT und ein Dump. • Force Power Off: Erzwingt das Ausschalten der Partition. • Not specified: Es wird für die Partition keine Aktion ausgeführt. Anmerkung: • Führen Sie ein INIT aus, um das Beenden von in der Partition ablaufenden Anwendungen zu erzwingen. Schließen Sie wichtige Anwendungen, bevor Sie ein INIT ausführen. Hängen Sie ferner nicht benötigte Dateisysteme vor einem INIT aus.

2.5.10 Partitionsinformationen anzeigen

Mit dieser Funktion können Sie Statusinformationen und sonstige Angaben zu einer Partition anzeigen.

Ferner können Sie im Fenster [Partition Configuration] die gesamte Partitionskonfiguration des PRIMEQUEST-Systems überprüfen.

Vorgehensweise

1 Wählen Sie [Partition] → [Partition#x] → [Information]
Das Fenster [Information] wird angezeigt.

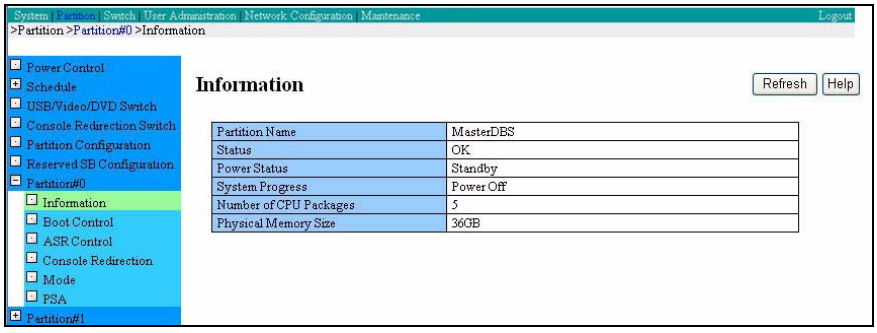


Abbildung 2.50 Das Fenster [Information]

Tabelle 2.29 Feldnamen und mögliche Eingaben im Fenster [Information]

Feldname	Beschreibung
Partition Name	Name der Partition.
Status	Status der Partition. • OK: Die Partition funktioniert ordnungsgemäß. • Degraded: In der Partition ist eine Komponente ausgefallen (die ausgefallene Komponente wurde isoliert). • Warning: Die Partition wird vermutlich in naher Zukunft ausfallen. • Failed: Die Partition ist ausgefallen.
Power Status	Einschaltstatus der Partition. • On: Die Partition ist eingeschaltet. • Standby: Die Partition befindet sich im Standby-Zustand.

Tabelle 2.29 Feldnamen und mögliche Eingaben im Fenster [Information]

Feldname	Beschreibung
System Progress	Fortschritt der Partition. • [Power Off]: Die Partition ist ausgeschaltet. • [Power On In Progress]: Die Partition wird eingeschaltet. • [Reset]: Die Partition wird neu gestartet. • [POST XXXXh]: Der Vorgang POST Code=XXXXh hat begonnen. • Boot: Die Partition hat einen der folgenden Zustände: - Die Partition wird hochgefahren. - SA ist nicht installiert - Installation läuft - Backup oder Sicherung mit dem Systemcast Wizard läuft. • [OS Running]: Das Betriebssystem läuft. • [OS Shutdown]: Das Betriebssystem ist heruntergefahren. • [Panic]: Die Partition befindet sich im Panic-Modus. • [Power Off In Progress]: Die Partition wird ausgeschaltet. • [Check Stop]: Die Partition ist ausgeschaltet.
Number of CPU packages	Gibt die Anzahl der in der Partition enthaltenen CPU-Pakete an. Hinweis: Fehlerhafte CPUs sind in dieser Zahl nicht enthalten.
Physical Memory Size	Gibt die physikalische Speichergröße der Partition an. Hinweis: Dieser Wert weicht von der Speichergröße ab, die das Betriebssystem tatsächlich nutzen kann. Fehlerhafte DIMMs sind in der Angabe nicht enthalten.

2.6 Konfiguration sichern

Dieser Abschnitt beschreibt, wie Sie erstellt Konfiguration sichern können. Stellen Sie sicher, dass immer eine Sicherung der aktuellen MMB-Konfigurationsinformationen existiert.

- MMB-Konfigurationsdaten sichern (→ 2.6.1)

Anmerkungen:

- Wie Sie die PSA-Informationen und EFI-Einstellungen sichern können, ist in Abschnitt 4.13, „Konfigurationsdaten sichern“, in Kapitel 4, „Nach Installation des Betriebssystems erforderliche Arbeiten“ beschrieben.
- Machen Sie in regelmäßigen Abständen eine Sicherung der MMB-Konfigurationsinformationen.

2.6.1 MMB-Konfigurationsdaten sichern

In diesem Abschnitt wird beschrieben, wie Sie die MMB-Konfigurationsdaten sichern können. Die MMB-Konfigurationsdaten werden auf einem entfernten PC gesichert.

Anm.: Weitere Einzelheiten zur Sicherung der MMB-Konfigurationsdaten finden Sie im Abschnitt 5.6.2.1, „[Backup/Restore Configuration] window“ des *PRIMEQUEST 580A/540A/520A/500/400 Series Reference Manual: Basic Operation/GUI/Commands* (U41633-J-Z816-x-76/C122-E003EN).

Verfahren

1 Wählen Sie [Maintenance] → [Backup/Restore Configuration] → [Backup/Restore MMB Configuration].
Das Fenster [Backup MMB Configuration] wird angezeigt.

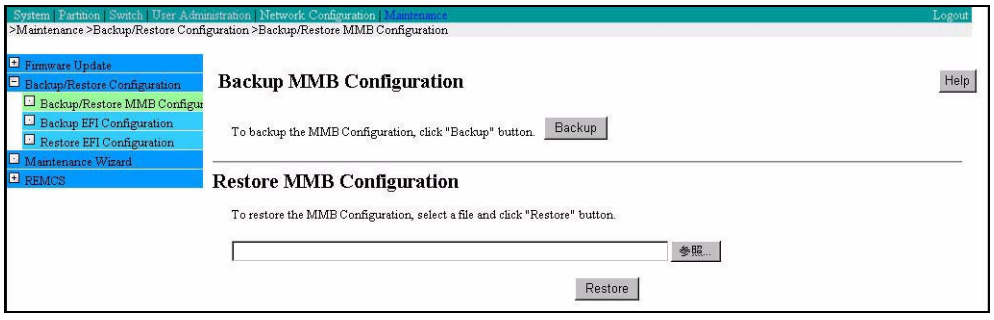


Abbildung 2.51 Das Fenster [Backup MMB Configuration]

2 Klicken Sie auf die Schaltfläche [Backup].
Sie können das Ziel für die Konfigurationssicherung mithilfe der Browse-Schaltfläche auswählen.

3 Wählen Sie das Ziel aus und klicken Sie auf [OK].
Damit wird die Konfigurationsdatei zum angegebenen Ziel heruntergeladen.
Der Standardname der MMB-Konfigurationsdatei lautet:

```
MMB_(backup-date)_(MMB-version).dat
```

KAPITEL 3 Betriebssystem installieren

3.1 Überblick

In diesem Abschnitt werden die folgenden Themen beschrieben:

- Unterstützte Betriebssysteme (→ 3.1.1)
- Installationsverfahren (→ 3.1.2)
- Installationsvoraussetzungen (→ 3.1.3)
- Nach Installation des Betriebssystems erforderliche Arbeiten (→ 3.1.4)

3.1.1 Unterstützte Betriebssysteme

Folgende Betriebssysteme werden unterstützt:

- Red Hat® Enterprise Linux® AS (V.4 für Itanium)
- Red Hat® Enterprise Linux® 5 (für Intel Itanium)
- SUSE™ Linux Enterprise Server 9 für Itanium-basierte Systeme
- SUSE™ Linux Enterprise Server 10 for Itanium-basierte Systeme
- Microsoft® Windows Server® 2003, Enterprise Edition für Itanium-basierte Systeme
- Microsoft® Windows Server® 2003, Datacenter Edition für Itanium-basierte Systeme
- Microsoft® Windows Server® 2008 for Itanium-Based Systems

3.1.2 Installationsverfahren

In diesem Abschnitt werden die verschiedenen Verfahren zur Installation der Linux und Windows Betriebssysteme beschrieben. Ferner wird auf die Unterschiede zwischen ihnen hingewiesen.

Installationsverfahren für Linux

Das Linux Betriebssystem kann wie folgt installiert werden:

- Lokale Installation: Linux OS installation über die KVM-Einheit (PRIMEQUEST 580A/540A*/580/540/480/440) Installation über unabhängigen KVM-Switch (PRIMEQUEST 520A*/520/420)
- Entfernte Installation: Installation mit SystemcastWizard Lite

Anm.: Verwenden Sie das entfernte Installationsverfahren, wenn Sie das Betriebssystem auf mehreren Partitionen installieren wollen.

Tabelle 3.1 zeigt die Unterschiede zwischen den beiden Verfahren auf.

Tabelle 3.1 Vergleich der Installationsverfahren für Linux

Art	Verfahren	Server-Konfiguration	Gleichzeitige Installation mehrerer Partitionen	Benutzer-freundlichkeit
Lokale Installation	Installation über KVM	Bildschirm, USB-Tastatur, USB-Maus und USB-Diskettenlaufwerk an der KVM-Einheit angeschlossen	Nicht zulässig	Hoch
	Installation ohne KVM	Bildschirm, USB-Tastatur, USB-Maus und USB-Diskettenlaufwerk am Server angeschlossen		
Entfernte Installation	Installation mit SystemcastWizard Lite	Installationsserver und SystemcastWizard Lite erforderlich	Zulässig	Hoch

*: wird von Fujitsu Technology Solutions nicht unterstützt

Installationsverfahren für Windows

Das Windows Betriebssystem kann wie folgt installiert werden:

- Entfernte Installation:
  Installation mit SystemcastWizard Lite
- Lokale Installation:
  - Installation mit Hilfe des Installation Support Tool für Windows
  - Installation über eine KVM-Einheit

Tabelle 3.2 zeigt die Unterschiede zwischen den beiden Verfahren auf.

Tabelle 3.2 Vergleich der Installationsverfahren für Windows

Art	Verfahren	Empfehlungsgrad	Gleichzeitige Installation mehrerer Partitionen	Benutzer-freundlich-keit	Verbindung mit PRIMEQUEST Software Installer
Entfernte Installation	Installation mit SystemcastWizard Lite remote	sehr	verfügbar	O	verfügbar
Lokale Installation	Installation mit Installation Support Tool für Windows	mittel	nicht verfügbar	O	verfügbar
Lokale Installation	Händische Installation über KVM	selten	nicht verfügbar	-	nicht verfügbar

- Entfernte Installation mit SystemcastWizard Lite (empfohlen)

  Die Software SystemcastWizard Lite, die mit dem PRIMEQUEST-System ausgeliefert wird, dient zur Installation von Windows. Sie ermöglicht eine automatisierte Installation in einem Netzwerk.

  Im Anschluss an Windows werden automatisch Tools zur Erhöhung der Betriebszuverlässigkeit installiert.

  Einzelheiten finden Sie in Abschnitt 3.3.2, „Windows mit SystemcastWizard Lite installieren“.

- Installation Support Tool für Windows

  Das Installation Support Tool, das mit dem PRIMEQUEST-System ausgeliefert wird, dient zur Installation von Windows. Die meisten Installationsschritte laufen automatisiert ab, mit Ausnahme des Wechseln von CD-ROMs/DVDs und einigen anderen Arbeiten.

  Im Anschluss an Windows werden automatisch Tools zur Erhöhung der Betriebszuverlässigkeit installiert.

Einzelheiten finden Sie in Abschnitt 3.3.3, „Installation von Windows mit dem Installation Support Tool“.

- Händische Installation mit KVM

  Windows wird im Dialog mit dem Benutzer von DVD installiert.

  Im Anschluss an Windows müssen die Tools zur Erhöhung der Betriebszuverlässigkeit von Hand installiert werden.

  Einzelheiten finden Sie in Section 3.3.4, „Installation von Windows mit KVM (PRIMEQUEST 580A/540A/580/540/480/440)“ und Abschnitt 3.3.5, „Installation von Windows mit unabhängigem KVM-Switch (PRIMEQUEST 520A/520/420)“.

3.1.3 Installationsvoraussetzungen

Das Betriebssystem muss in jeder Partition installiert werden.

Hierfür müssen folgende Voraussetzungen gegeben sein:

- Die in Kapitel 2, „Installation“, beschriebenen Aufgaben wurden ausgeführt.
  - Die PRIMEQUEST Systemeinheit ist installiert.
  - Die Servereinheit ist installiert.
  - Die MMB-Konsole ist angeschlossen und steuert das MMB.
  - Die benötigten Partitionen sind bereits eingerichtet.
- Alle für die Installation des Betriebssystems (LINUX bzw. Windows) erforderlichen Mittel liegen vor.
  - Installationsmedium
  - Serverlizenz
  - CAL (Windows)

3.1.4 Nach Installation des Betriebssystems erforderliche Arbeiten

Nachdem Sie das Betriebssystem installiert haben, müssen die in Tabelle 3.3 genannten Aufgaben durchgeführt werden. Diese Aufgaben werden in Kapitel 4, „Nach Installation des Betriebssystems erforderliche Arbeiten“ im Einzelnen beschrieben.

Tabelle 3.3 Aufgaben nach der Installation

Betriebssystem	Aufgabe	Beschreibung
Linux oder Windows	PSA einrichten	Die PSA-Einstellungen müssen gemacht werden. S.M.A.R.T. muss eingerichtet werden. Watchdog muss eingerichtet werden.
Linux oder Windows	NTP-Client einrichten	Ein NTP-Client muss eingerichtet werden.
Linux (nur Red Hat) oder Windows	Dump-Umgebung einrichten	Eine Dump-Umgebung muss eingerichtet werden.
Linux (nur Red Hat) oder Windows	BS-Sicherung erstellen	Das installierte Betriebssystem muss gesichert werden.
Linux oder Windows	Einstellungen sichern	Die PSA- und EFI-Einstellungen müssen gesichert werden.

Anm.: Die betriebssystemnahen Komponenten für die Ausführung des REMCS* werden bei der Installation von PSA unter Linux (Red Hat) oder Windows installiert. Die REMCS*-Konfiguration wird von einem Kundendienst-Techniker durchgeführt.

*: wird von Fujitsu Technology Solutions nicht unterstützt

3.2 Installation des Betriebssystems Linux

In diesem Abschnitt werden die folgenden Installationsverfahren beschrieben:

- Linux Installation über KVM (PRIMEQUEST 580A/540A/580/540/480/440) (→ 3.2.1)
- Unabhängigen KVM-Switch für die Installation des Linux-Betriebssystems verwenden (PRIMEQUEST 520A/520/420) (→ 3.2.2)
- Installation mit SystemcastWizard Lite (→ 3.2.3)

Für eine effiziente Installation mehrerer Systeme (drei oder mehr Systempartitionen) wird der Einsatz von SystemcastWizard Lite empfohlen.

3.2.1 Linux Installation über KVM (PRIMEQUEST 580A/540A*/580/540/480/440)

3.2.1.1 Hardwarevoraussetzungen und Vorgehensweise

Bevor Sie das Betriebssystem über die KVM-Einheit installieren, müssen Sie eine config-Datei erstellen. Diese enthält Optionseinstellungen für die Installation etc. Erstellen Sie die config-Datei mithilfe des Installation Support Tools.

Tabelle 3.4 gibt einen Überblick über die Voraussetzungen für die Nutzung des Installation Support Tools. Weitere Einzelheiten finden Sie im *PRIMEQUEST Installation Support Tool User's Guide (Red Hat)* (C122-E005EN) oder im *PRIMEQUEST Installation Support Tool User's Guide (SUSE)* (C122-E047EN).

Tabelle 3.4 Voraussetzungen für das Installation Support Tool

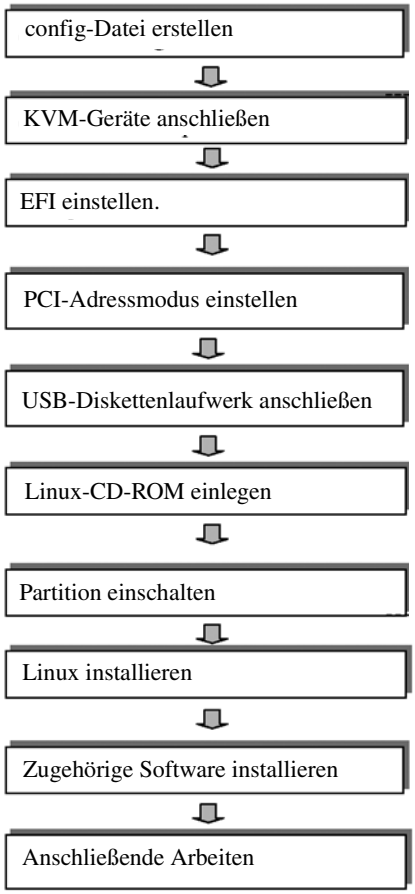
Bezeichnung	Voraussetzungen
Hardware	PC mit Windows Betriebssystem Eines der folgenden Betriebssysteme ist erforderlich*: • Windows 2000 Professional Service Pack4 oder höher • Windows XP Home Edition Service Pack2 oder höher • Windows XP Professional Service Pack2 oder höher * nur die 32-bit-Version der Betriebssysteme

*: wird von Fujitsu Technology Solutions nicht unterstützt

Wenn Sie die config-Datei erstellt haben, können Sie mit der Installation über die KVM-Einheit beginnen. Schließen Sie dazu die folgenden Geräte an:

- Bildschirm
- USB-Tastatur
- USB-Maus
- USB-Diskettelaufwerk

Die Installation umfasst folgende Schritte:



3.2.1.2 config-Datei für die Installation erstellen

Wählen Sie mit Hilfe des Tools die Installationsoptionen etc. aus. Weitere Einzelheiten finden Sie im *PRIMEQUEST Installation Support Tool User's Guide (Red Hat)* (C122-E005EN) oder im *PRIMEQUEST Installation Support Tool User's Guide (SUSE)* (C122-E047EN).

3.2.1.3 Geräte anschließen

Führen Sie folgende Schritte aus, um die KVM an die Partition anzuschließen, auf der Sie Linux installieren wollen:

(1) KVM anschließen

1 Schließen Sie eine Tastatur, eine Maus und einen Bildschirm an die KVM-Einheit an.

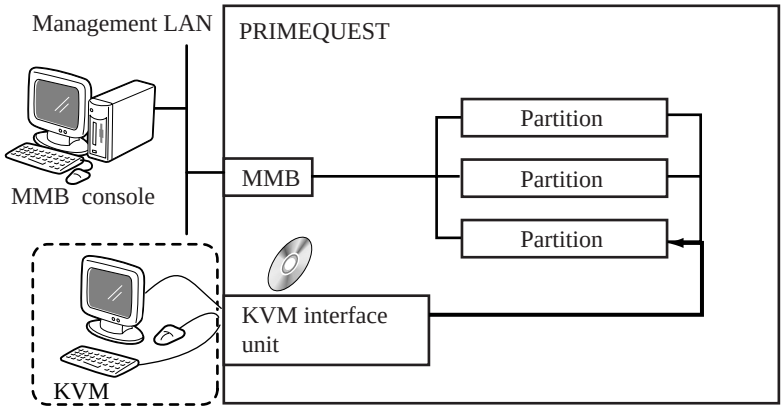


Abbildung 3.1 Anschlüsse für eine Installation über KVM

2 Wählen Sie in der MMB Web-UI [Partition] → [USB/Video/DVD Switch].
Das Fenster [USB/Video/DVD Switch] wird angezeigt.

Anm.: Im Abschnitt 2.2.2.1, „An- und Abmelden bei der MMB Web-UI“ ist beschrieben, wie Sie sich beim MMB Web-UI anmelden.

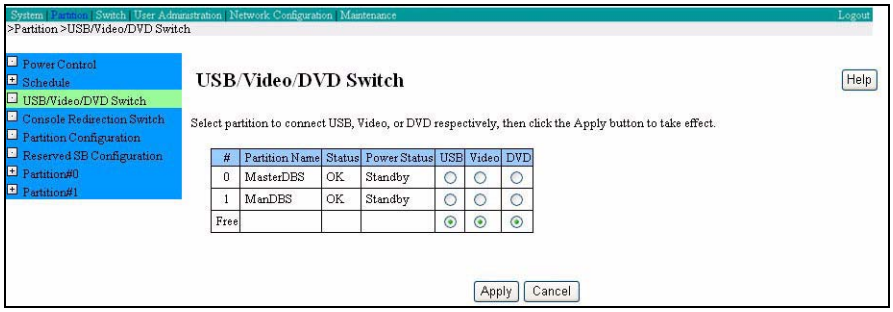


Abbildung 3.2 Das Fenster [USB/Video/DVD Switch]

3 Aktivieren Sie die USB-, Video- und DVD-Optionsfelder der Partition, auf der Sie das Betriebssystem installieren und klicken Sie dann auf die Schaltfläche [Apply].

(2) EFI einrichten

Richten Sie das EFI für die Partition ein, auf der Sie das Betriebssystem installieren wollen, damit der Rechner von der DVD-ROM hochgefahren wird.

1 Klicken Sie im Fenster MMB Web-UI auf [Partition] → [Partition#x] → [Boot Control].
Das Fenster [Boot Control] wird angezeigt.

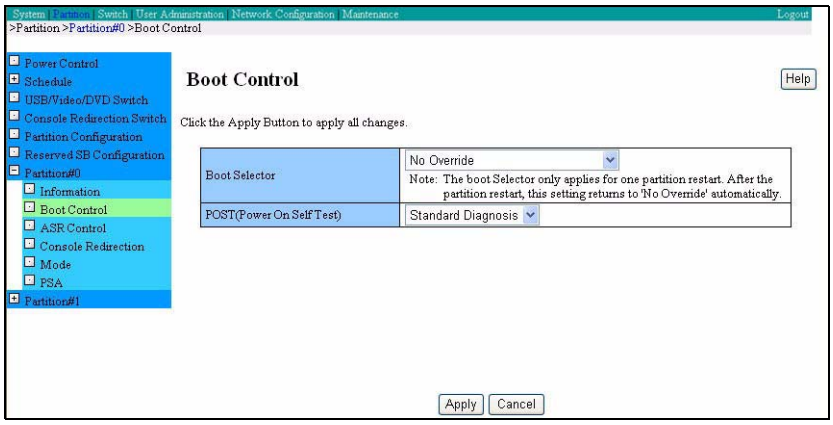


Abbildung 3.3 Das Fenster [Boot Control]

2 Wählen Sie bei [Boot Selector] die Option [Force boot from DVD] aus und klicken Sie dann auf die Schaltfläche [Apply].

(3) PCI Address Mode einstellen

Stellen Sie den „PCI Bus Mode“ als Adressierungsmodus der Partition ein, in der das Betriebssystem installiert werden soll.

1 Klicken Sie im Fenster MMB Web-UI auf [Partition] → [Partition #x] → [Mode]. Das Fenster [Mode] wird angezeigt.

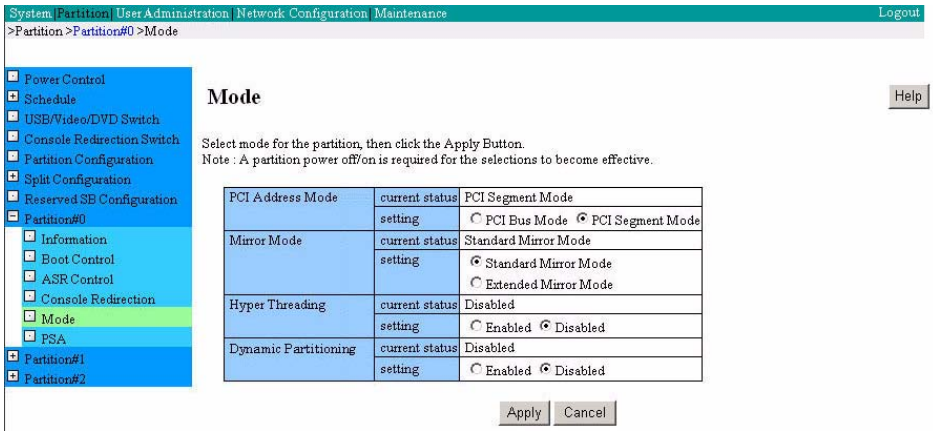
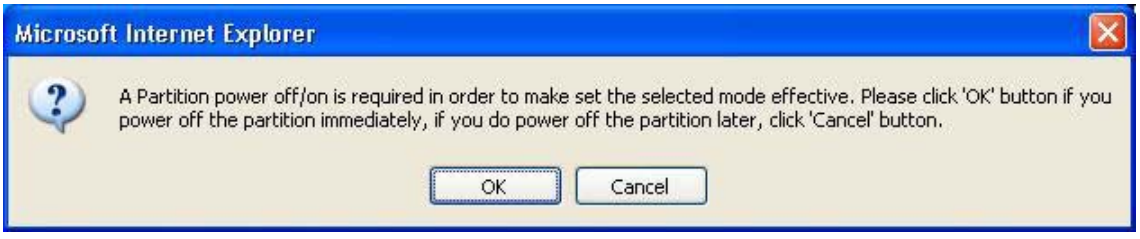


Abbildung 3.4 Fenster [Mode] (PRIMEQUEST 580A/540A*)

2 Wählen Sie bei [PCI Address Mode] die Option [PCI Bus Mode] und klicken Sie dann auf die Schaltfläche [Apply].


Microsoft Internet Explorer
A Partition power off/on is required in order to make set the selected mode effective. Please click 'OK' button if you power off the partition immediately, if you do power off the partition later, click 'Cancel' button.
OK
Cancel

Es wird ein Konfigurationsfenster angezeigt.

3 Klicken Sie auf [OK].

Bemerkung: Verwenden Sie PCI Bus Mode, so dass für die PRIMEQUEST eine feste Adresse im LAN gesetzt wird, die im MMB während der Installation registriert ist.

(4) USB-Diskettenlaufwerk anschließen

1 Schließen Sie an den USB-Port der KVM-Einheit ein USB-Diskettenlaufwerk an und legen Sie die Diskette mit der Konfigurationsdatei ein.

*: wird von Fujitsu Technology Solutions nicht unterstützt

(5) CD-ROM mit dem Linux Betriebssystem einlegen

1 Legen Sie im DVD-ROM-Laufwerk der KVM-Einheit die CD-ROM mit dem Linux-Betriebssystem ein.

(6) Partition einschalten

Schalten Sie die Partition wie im Folgenden beschrieben ein.

Wenn die Partition bereits eingeschaltet ist, dann starten Sie sie neu.

1 Klicken Sie im Fenster MMB Web-UI auf [Partition] → [Power Control]. Das Fenster [Power Control] wird angezeigt.

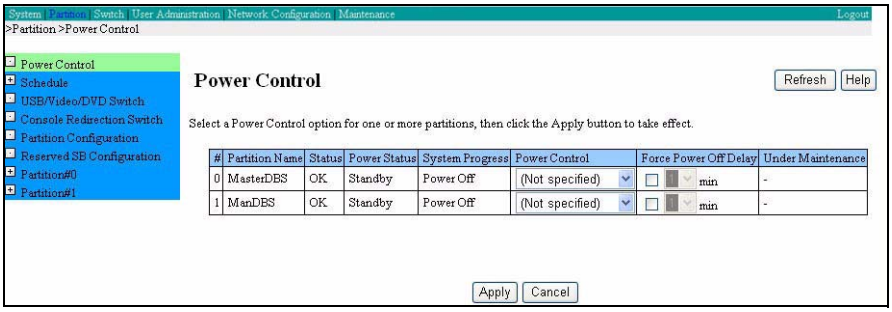

System | Partition | Switch | User Administration | Network Configuration | Maintenance
Logout
>Partition >Power Control
Power Control
Schedule
USB/Video/DVD Switch
Console Redirection Switch
Partition Configuration
Reserved SB Configuration
Partition#0
Partition#1
Power Control
Refresh
Help
Select a Power Control option for one or more partitions, then click the Apply button to take effect.
| Partition Name | Status | Power Status | System Progress | Power Control | Force Power Off Delay | Under Maintenance
0 | MasterDBS | OK | Standby | Power Off | (Not specified) | min | -
1 | ManDBS | OK | Standby | Power Off | (Not specified) | min | -
Apply
Cancel

Abbildung 3.5 Das Fenster [Power Control]

2 Wählen Sie im Feld [Power Control] der Partition, die Sie einschalten wollen, entweder die Option [Power On] oder [Reset].

3 Klicken Sie auf die Schaltfläche [Apply].

3.2.1.4 Linux Betriebssystem installieren

Booten Sie das Betriebssystem von der CD, um es zu installieren.

Weitere Einzelheiten finden Sie im *PRIMEQUEST Installation Support Tool User's Guide (Red Hat)* (C122-E005EN) oder im *PRIMEQUEST Installation Support Tool User's Guide (SUSE)* (C122-E047EN).

Folgen Sie den Anweisungen des Installers, die auf dem Bildschirm der KVM-Einheit angezeigt werden, um die CD-ROM zu wechseln. Wenn das Linux Betriebssystem vollständig installiert ist, wird das System neu gestartet.

Hinweis: Wenn die Partition, die an die KVM-Einheit angeschlossen ist, während der Installation des Linux-Betriebssystems gewechselt wird, wird der Installationsvorgang möglicherweise abgebrochen und es kommt zu einem I/O-Fehler. Ändern Sie nicht die KVM-Verbindung während einer Installation.

3.2.1.5 Zugehörige Softwareprogramme installieren

Folgen Sie nach der Installation des Betriebssystems den Anweisungen auf der KVM-Konsole, legen Sie die zum Lieferumfang gehörende CD-ROM in das DVD-ROM-Laufwerk, und installieren Sie die mitgelieferten Programme. Näheres über die Installation von Bundled-Software finden Sie im *PRIMEQUEST Installation Support Tool User's Guide (Red Hat)* (C122-E005EN) oder im *PRIMEQUEST Installation Support Tool User's Guide (SUSE)* (C122-E047EN).

3.2.1.6 Nach der Installation erforderliche Aufgaben

Ziehen Sie nach Abschluss der Installation das USB-Kabel zur USB-Floppy aus dem USB-Port am KVM. Stellen Sie anschließend den PCI Address Mode ein.

Stellen Sie für die Partition, in der das Betriebssystem installiert wurde, „PCI Segment Mode“ als PCI Address Mode ein. Informationen zum Einstellvorgang finden Sie in 2.5.8, „Verschiedene Modes einstellen“.

Führen Sie nach der Einstellung des PCI Address Mode die für das Linux-Betriebssystem erforderlichen Arbeiten aus. Eine genaue Beschreibung finden Sie in KAPITEL 4, „Nach Installation des Betriebssystems erforderliche Arbeiten“.

3.2.2 Unabhängigen KVM-Switch für die Installation des Linux-Betriebssystems verwenden (PRIMEQUEST 520A*/520/420)

3.2.2.1 Hardware-Voraussetzungen und Vorgehensweise

Bevor Sie installieren können, müssen Sie eine config-Datei erzeugen. Eine config-Datei enthält Optionseinstellungen für das Betriebssystem etc. Benutzen Sie das Installation Support Tool, um eine config-Datei zu erzeugen.

Tabelle 3.5 enthält einen Überblick über die für den Einsatz des Installation Support Tools erforderlichen Systemvoraussetzungen. Weitere Einzelheiten finden Sie im *PRIMEQUEST Installation Support Tool User's Guide (Red Hat)* (C122-E005EN) oder im *PRIMEQUEST Installation Support Tool User's Guide (SUSE)* (C122-E047EN).

Tabelle 3.5 Systemvoraussetzungen des Installation Support Tools

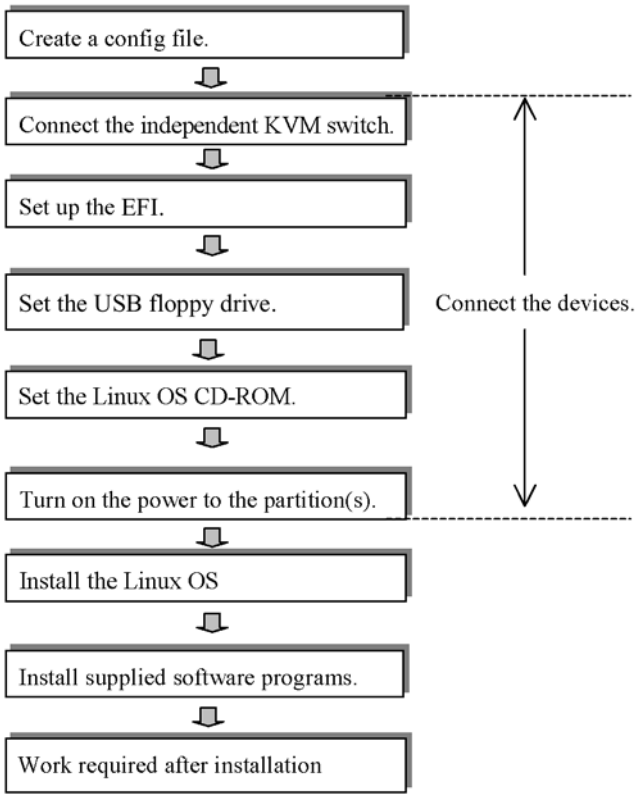
Bezeichnung	Voraussetzungen
Hardware	Windows-PC Eines der folgenden Betriebssysteme ist erforderlich*: • Windows 2000 Professional Service Pack4 oder höher • Windows XP Home Edition Service Pack2 oder höher • Windows XP Professional Service Pack2 oder höher * Nur 32-Bit Versionen der Betriebssysteme

Wenn Sie die config-Datei erstellt haben, benötigen Sie für die Installation die folgenden Geräte:

- Bildschirm
- USB-Tastatur
- USB-Maus
- USB-Diskettelaufwerk

*: wird von Fujitsu Technology Solutions nicht unterstützt

Die Installation umfasst folgende Schritte:


Create a config file.
Connect the independent KVM switch.
Set up the EFI.
Set the USB floppy drive.
Set the Linux OS CD-ROM.
Turn on the power to the partition(s).
Install the Linux OS
Install supplied software programs.
Work required after installation
Connect the devices.

3.2.2.2 config-Datei für die Installation erstellen

Legen Sie mithilfe des Installation Support Tools die gewünschten Betriebssystem-Einstellungen fest etc. Weitere Einzelheiten finden Sie im *PRIMEQUEST Installation Support Tool User's Guide (Red Hat)* (C122-E005EN) oder im *PRIMEQUEST Installation Support Tool User's Guide (SUSE)* (C122-E047EN)

3.2.2.3 Geräte anschließen

Führen Sie folgende Schritte aus, um die für die Installation erforderlichen Geräte an die Partition anzuschließen, auf der Sie Linux installieren wollen:

(1) Unabhängigen KVM-Switch anschließen

1 Schließen Sie den unabhängigen KVM-Switch an den USB-Port einer IO Unit an.

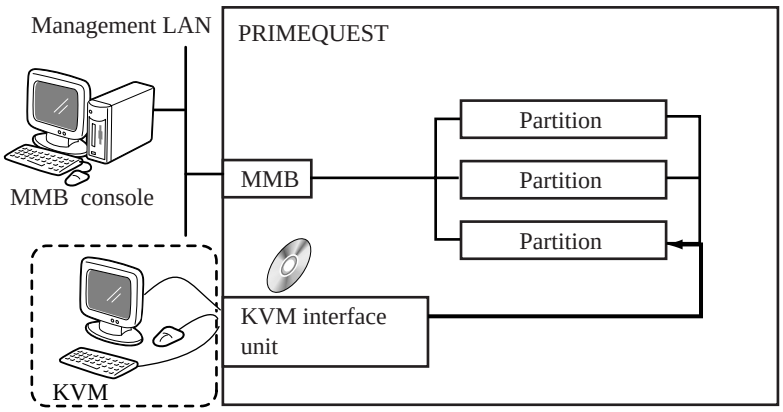


Abbildung 3.6 Anschlüsse für eine Installation über unabhängigen KVM-Switch

2 Klicken Sie im MMB Web-UI auf [Partition] → [DVD Switch].
Das Fenster [DVD Switch] wird angezeigt.
Anm.: Im 2.2.2.1, „An- und Abmelden bei der MMB Web-UI“ wird beschrieben, wie Sie sich beim MMB anmelden.

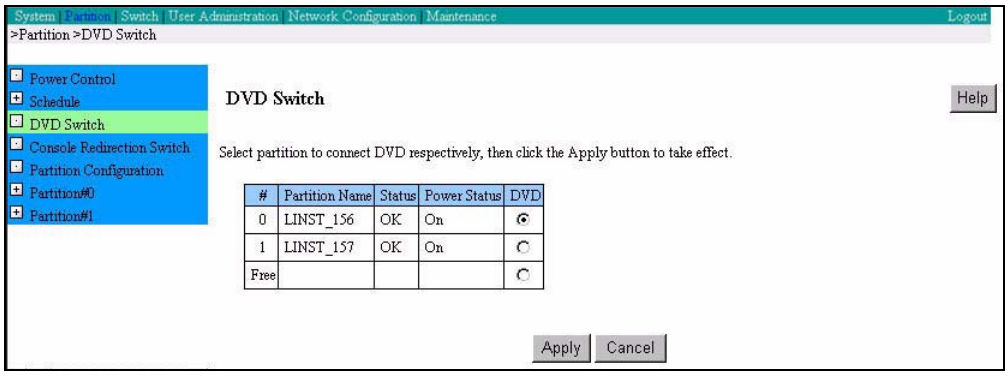


Abbildung 3.7 Das Fenster [DVD Switch]

3 Aktivieren Sie das DVD-Optionsfeld der Partition, auf der Sie das Betriebssystem installieren wollen und klicken Sie dann auf [Apply], um die Auswahl zu bestätigen.

(2) EFI einrichten

Richten Sie das EFI für die betreffende Partition so ein, dass das System von der DVD-ROM gestartet wird.

1 Wählen Sie im MMB Web-UI-Fenster [Partition] → [Partition#x] → [Boot Control].
Das Fenster [Boot Control] wird angezeigt.

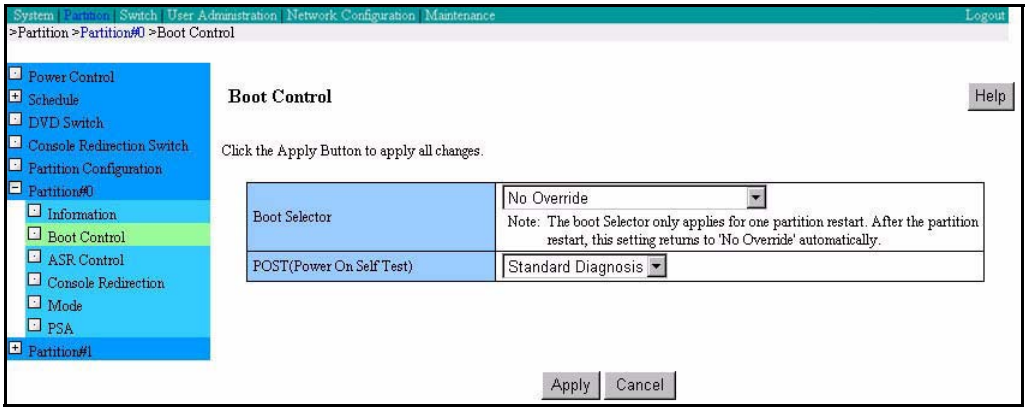


Abbildung 3.8 Das Fenster [Boot Control]

2 Wählen Sie bei [Boot Selector] die Option [Force boot from DVD] aus und klikken Sie auf [Apply], um Ihre Auswahl zu bestätigen.

(3) USB-Diskettenlaufwerk anschließen

1 Schließen Sie ein USB-Diskettenkaufwerk an den USB-Port des MMBs an.
Legen Sie dann die Diskette mit der Konfigurationsdatei in das Laufwerk ein.

(4) CD-ROM mit dem Linux Betriebssystem einlegen

1 Legen Sie die CD-ROM mit dem Linux Betriebssystem in das DVD-ROM-Laufwerk des OPL ein.

(5) Partition einschalten

Schalten Sie die Partition wie im Folgenden beschrieben ein.

Wenn die Partition bereits eingeschaltet ist, ist ein Neustart erforderlich.

1 Wählen Sie im MMB Web-UI [Partition] → [Power Control].
Das Fenster [Power Control] wird angezeigt.

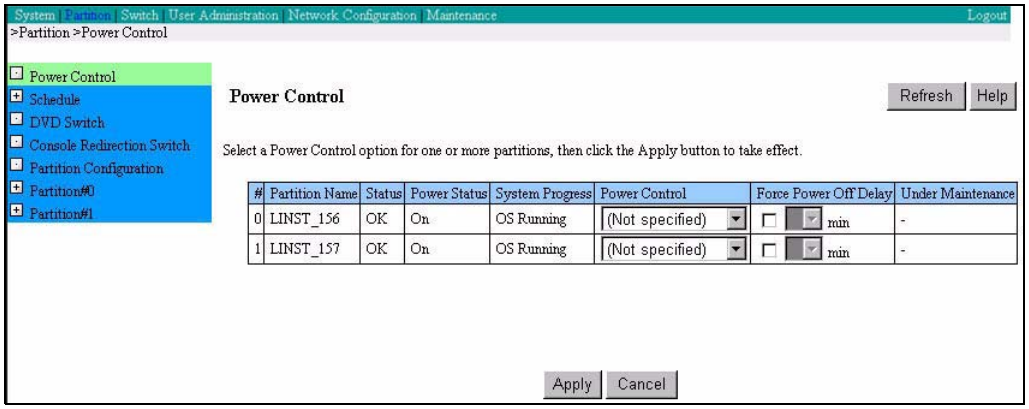

System | Partition | Switch | User Administration | Network Configuration | Maintenance
Logout
>Partition >Power Control
Power Control
Schedule
DVD Switch
Console Redirection Switch
Partition Configuration
Partition#0
Partition#1
Power Control
Refresh
Help
Select a Power Control option for one or more partitions, then click the Apply button to take effect.
Partition Name Status Power Status System Progress Power Control Force Power Off Delay Under Maintenance
0 LINST_156 OK On OS Running (Not specified) min -
1 LINST_157 OK On OS Running (Not specified) min -
Apply
Cancel

Abbildung 3.9 Das Fenster [Power Control]

2 Wählen Sie unter [Power Control] für die Partition, die eingeschaltet werden soll, die Option [Power On] aus.
Anm.: Ist die Partition bereits eingeschaltet, wählen Sie [Reset]

3 Klicken Sie dann auf [Apply].

3.2.2.4 Linux Betriebssystem installieren

Booten Sie das Betriebssystem von der CD.

Weitere Einzelheiten finden Sie im *PRIMEQUEST Installation Support Tool User's Guide (Red Hat)* (C122-E005EN) oder im *PRIMEQUEST Installation Support Tool User's Guide (SUSE)* (C122-E047EN).

Folgen Sie den Anweisungen des Installationsprogramms, um die CD-ROM zu wechseln. Wenn das Linux Betriebssystem vollständig installiert ist, wird das System neu gestartet.

3.2.2.5 Zugehörige Softwareprogramme installieren

Folgen Sie nach Installation des Betriebssystems den auf der KVM-Konsole angezeigten Anweisungen, legen Sie die zum Lieferumfang gehörende CD-ROM in das DVD-ROM-Laufwerk des OPL ein und installieren Sie die Softwareprogramme.

Weitere Einzelheiten finden Sie im *PRIMEQUEST Installation Support Tool User's Guide (Red Hat)* (C122-E005EN) oder im *PRIMEQUEST Installation Support Tool User's Guide (SUSE)* (C122-E047EN).

3.2.2.6 Nach der Installation erforderliche Aufgaben

Ziehen Sie nach Abschluss der Installation das USB-Kabel zur USB-Floppy aus dem USB-Port am KVM. Führen Sie jetzt die nach der Installation des Linux-Betriebssystems erforderlichen Aufgaben durch.

Weitere Informationen finden Sie in 3.1.4, „Nach Installation des Betriebssystems erforderliche Arbeiten“.

3.2.3 Installation mit SystemcastWizard Lite

3.2.3.1 Hardwarevoraussetzungen und Vorgehensweise

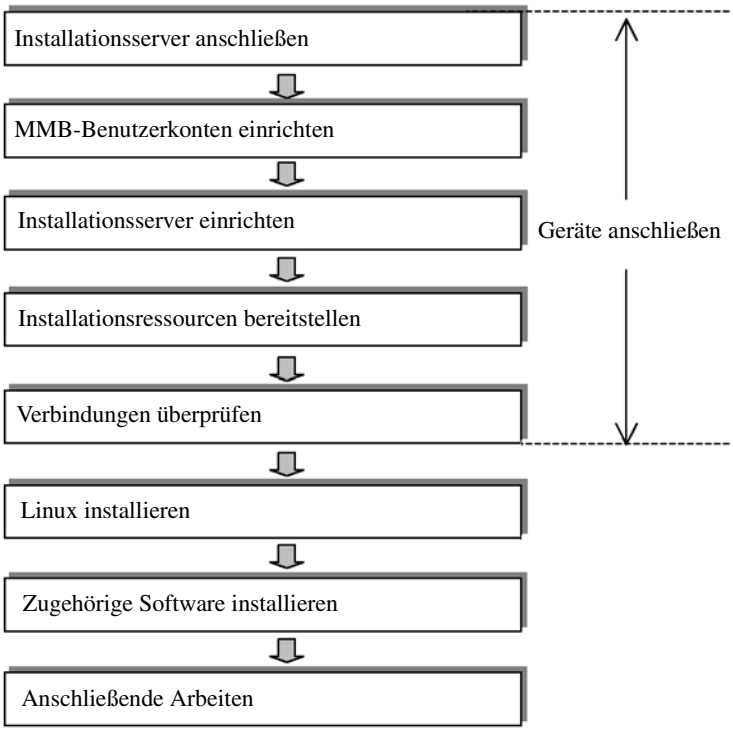
Bevor Sie das Betriebssystem mit SystemcastWizard Lite installieren können, müssen Sie einen PC entsprechend vorbereiten. Installieren Sie SystemcastWizard Lite auf einem PC und benutzen Sie diesen als Installationsserver, auf dem die erforderlichen registrierten Ressourcen und Informationen gespeichert werden können.

Tabelle 3.6 enthält einen Überblick über die Systemvoraussetzungen. Weitere Einzelheiten finden Sie im *PRIMEQUEST SystemcastWizard Lite User's Guide* (C122-E010EN).

Tabelle 3.6 Systemvoraussetzungen im Überblick

Komponente	Voraussetzungen
Hardware	PRIMERGY/FMV Serie (IA-32) Ein CD-ROM- oder DVD-Laufwerk ist erforderlich. Eines der folgenden Betriebssysteme ist erforderlich: • Windows Server 2003, Standard Edition (Service Pack 1 oder höher) • Windows Server 2003, Enterprise Edition (Service Pack 1 oder höher) • Windows Server 2003 R2, Standard Edition • Windows Server 2003 R2, Enterprise Edition • Windows XP Professional (Service Pack 2 oder höher) • Windows Vista Business • Windows Vista Enterprise
	LAN-Kabel
Software	SystemcastWizard Lite, PRIMEQUEST Software-Bundle-Package

Die Installation umfasst folgende Schritte:



3.2.3.2 Geräte anschließen

Schließen Sie die Geräte wie folgt an:

(1) Installationsserver

1 Schließen Sie den Installationsserver an das Netzwerk an.
Eine Beschreibung der Installation von SystemcastWizard Lite finden Sie im *PRIMEQUEST SystemcastWizard Lite User's Guide* (C122-E010EN).

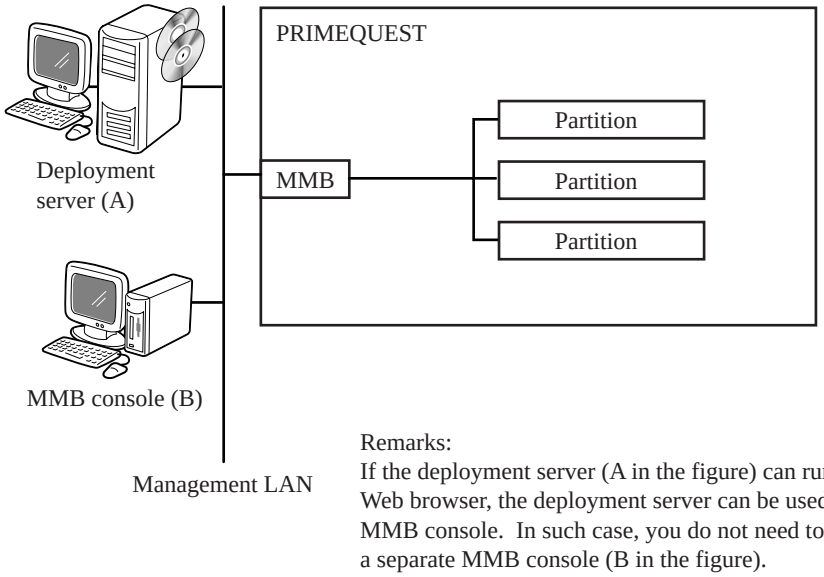

PRIMEQUEST
Partition
Partition
Partition
MMB
Deployment server (A)
MMB console (B)
Management LAN
Remarks:
If the deployment server (A in the figure) can run the Web browser, the deployment server can be used as the MMB console. In such case, you do not need to obtain a separate MMB console (B in the figure).

Abbildung 3.10 Anschlussbeispiel für die Installation mit SystemcastWizard Lite

Hinweis: Obwohl das Netzwerk mit PXE aktiviert ist, können Sie es nicht über einen Router aktivieren. Schließen Sie den Installationsserver daher an das Management-LAN an, an das auch die PRIMEQUEST angeschlossen ist.
Die Zielpartition wird entfernt gestartet oder das MMB#0 wird für die gesamte Kommunikation für Datensicherungen und -wiederherstellungen benutzt. Dazu sollten Sie das MMB#0 immer an das Management-LAN angeschlossen haben, es muss allerdings nicht aktiv sein.

(2) Benutzerkonten für den Zugriff auf das MMB einrichten

Sie können die für die entfernte Steuerung des MMB mit RMCP erforderlichen Benutzerdaten festlegen.

1 Wählen Sie [Network Configuration] → [Remote Server Management] im MMB Web-UI. Das Fenster [Remote Server Management] wird angezeigt.

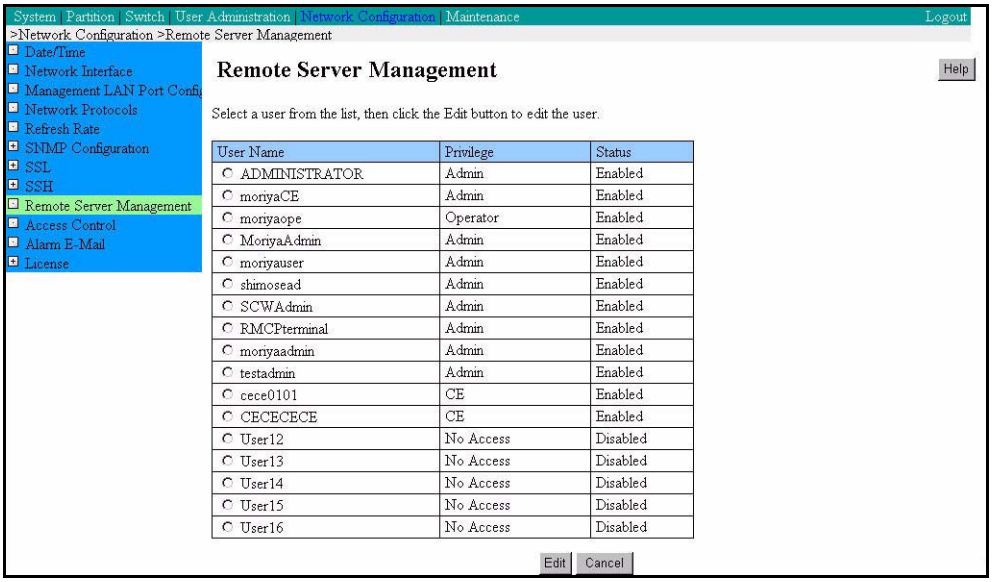


Abbildung 3.11 Das Fenster [Remote Server Management] (Beispiel)

2 Wählen Sie den betreffenden Benutzer aus, indem Sie das dazugehörige Optionsfeld anklicken und klicken Sie dann auf die Schaltfläche [Edit].
Das Fenster [Edit User] wird angezeigt.

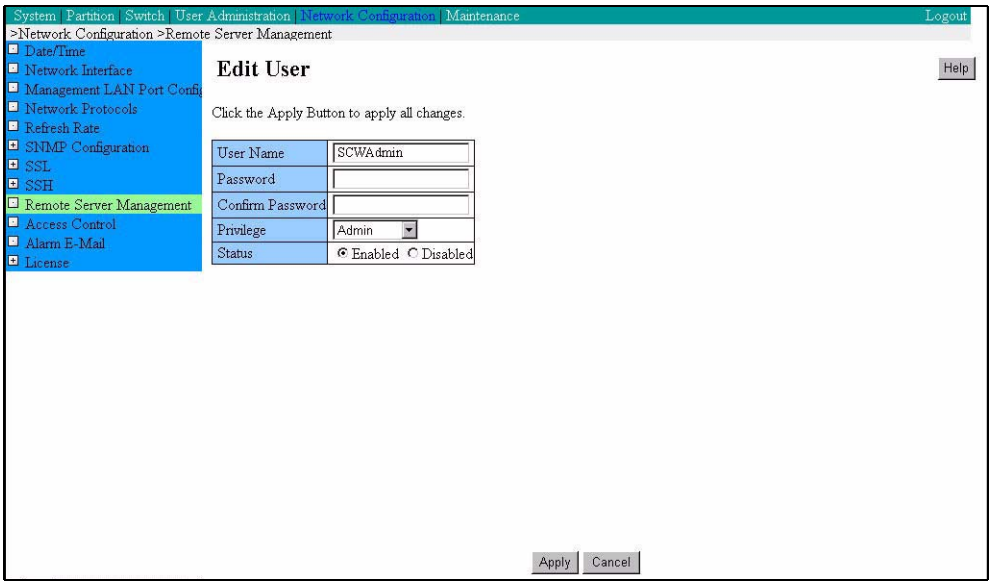


Abbildung 3.12 Das Fenster [Edit User] (Beispiel)

3 Geben Sie im Fenster [Edit User] die Benutzerverwaltungsdaten ein und klicken Sie auf [Apply], um die Eingaben zu bestätigen.
- User Name: Geben Sie einen Benutzernamen ein (8 bis 16 Zeichen).
- Password: Geben Sie ein Kennwort ein (8 bis 16 Zeichen).
- Confirm Password: Wiederholen Sie das Kennwort zur Bestätigung.
- Privilege: Wählen Sie aus der Dropdown-Liste Admin aus.
- Status: Wählen Sie die Option Enabled.

(3) Installationsserver einrichten

1 Registrieren Sie die Partition, auf der Sie Linux installieren wollen, auf dem Installationsserver. Benutzen Sie dazu die graphische Bedienoberfläche (Installationskonsole) des SystemcastWizard Lite. Einzelheiten finden Sie im *PRIMEQUEST SystemcastWizard Lite User's Guide* (C122-E010EN).

(4) Ressourcen für die Installation bereitstellen

Eine genaue Beschreibung der für die Installation mit SystemcastWizard Lite erforderlichen Ressourcen finden Sie im *PRIMEQUEST SystemcastWizard Lite User's Guide* (C122-E010EN).

(5) Verbindungen überprüfen

Überprüfen Sie, ob Sie vom Installationsserver auf folgende Dienste zugreifen können:

- TFTP - Starten des Netzwerks
- FTP - Installation des Betriebssystems in einer Netzwerkumgebung
- DHCP- Zuweisung einer IP-Adresse zu jeder PRIMEQUEST-Partition und Überprüfung der Konfiguration des Dienstes

3.2.3.3 Linux installieren

Legen Sie auf der Installationskonsole die Ressourcen an und installieren Sie Linux. Einzelheiten finden Sie im *PRIMEQUEST SystemcastWizard Lite User's Guide* (C122-E010EN).

3.2.3.4 Software-Bundle-Package installieren

Das Software-Bundle-Package wird vom SystemcastWizard Lite nach der Installation des Betriebssystems installiert. PSA wird ebenfalls zu diesem Zeitpunkt installiert.

3.2.3.5 Nach der Installation erforderliche Aufgaben

- PRIMEQUEST 580A/540A*/580/540/480/440

  Stellen Sie nach der Installation den PCI Address Mode ein.

  Stellen Sie für die Partitionen, in denen das Betriebssystem installiert wurde, „PCI Segment Mode“ als PCI Address Mode ein. Das Vorgehen hierbei ist in Abschnitt 2.5.8, „Verschiedene Modes einstellen“ beschrieben.

  Führen Sie nach der Einstellung des PCI Address Mode die für das Linux-Betriebssystem erforderlichen Arbeiten aus. Eine genaue Beschreibung finden Sie in KAPITEL 4, „Nach Installation des Betriebssystems erforderliche Arbeiten“.

- PRIMEQUEST 520A*/520/420

  Führen Sie die für das Linux-Betriebssystem erforderlichen Arbeiten aus. Eine genaue Beschreibung finden Sie in KAPITEL 4, „Nach Installation des Betriebssystems erforderliche Arbeiten“.

*: wird von Fujitsu Technology Solutions nicht unterstützt

3.3 Windows installieren

Um mit der PRIMEQUEST eine höchst verfügbare Umgebung einzurichten, wird die Nutzung einer SAN Boot Environment mit SAN-Speichereinheiten (z.B. ETERNUS*) empfohlen. Zur Einrichtung einer SAN Boot Environment müssen folgende Schritte ausgeführt werden:

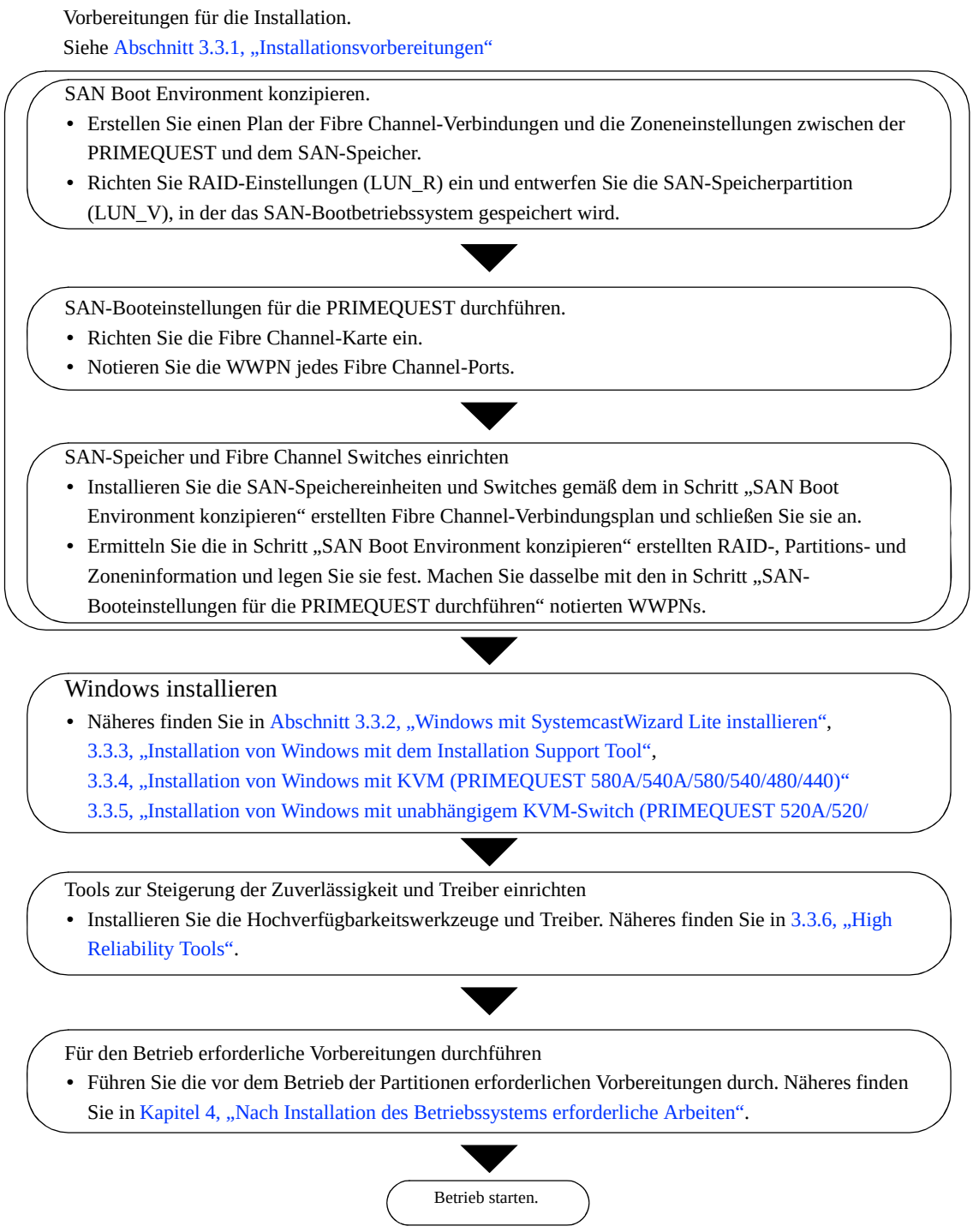

Vorbereitungen für die Installation.
Siehe Abschnitt 3.3.1, „Installationsvorbereitungen“
SAN Boot Environment konzipieren.
• Erstellen Sie einen Plan der Fibre Channel-Verbindungen und die Zoneneinstellungen zwischen der PRIMEQUEST und dem SAN-Speicher.
• Richten Sie RAID-Einstellungen (LUN_R) ein und entwerfen Sie die SAN-Speicherpartition (LUN_V), in der das SAN-Bootbetriebssystem gespeichert wird.
SAN-Booteinstellungen für die PRIMEQUEST durchführen.
• Richten Sie die Fibre Channel-Karte ein.
• Notieren Sie die WWPN jedes Fibre Channel-Ports.
SAN-Speicher und Fibre Channel Switches einrichten
• Installieren Sie die SAN-Speichereinheiten und Switches gemäß dem in Schritt „SAN Boot Environment konzipieren“ erstellten Fibre Channel-Verbindungsplan und schließen Sie sie an.
• Ermitteln Sie die in Schritt „SAN Boot Environment konzipieren“ erstellten RAID-, Partitions- und Zoneninformation und legen Sie sie fest. Machen Sie dasselbe mit den in Schritt „SAN-Booteinstellungen für die PRIMEQUEST durchführen“ notierten WWPNs.
Windows installieren
• Näheres finden Sie in Abschnitt 3.3.2, „Windows mit SystemcastWizard Lite installieren“, 3.3.3, „Installation von Windows mit dem Installation Support Tool“, 3.3.4, „Installation von Windows mit KVM (PRIMEQUEST 580A/540A/580/540/480/440)“ 3.3.5, „Installation von Windows mit unabhängigem KVM-Switch (PRIMEQUEST 520A/520/
Tools zur Steigerung der Zuverlässigkeit und Treiber einrichten
• Installieren Sie die Hochverfügbarkeitswerkzeuge und Treiber. Näheres finden Sie in 3.3.6, „High Reliability Tools“.
Für den Betrieb erforderliche Vorbereitungen durchführen
• Führen Sie die vor dem Betrieb der Partitionen erforderlichen Vorbereitungen durch. Näheres finden Sie in Kapitel 4, „Nach Installation des Betriebssystems erforderliche Arbeiten“.
Betrieb starten.

Abbildung 3.13 Arbeitsschritte für den Start des Systembetriebs

*: Angebot und Support in EMEA nur für die globalen Kunden von Fujitsu

In diesem Abschnitt werden die folgenden Schritte beschrieben:

- Installationsvorbereitungen (→ 3.3.1)
- Windows mit SystemcastWizard Lite installieren (→ 3.3.2)
- Installation von Windows mit dem Installation Support Tool (→ 3.3.3)
- Installation von Windows mit KVM (PRIMEQUEST 580A/540A/580/540/480/440) (→ 3.3.4)
- Installation von Windows mit unabhängigem KVM-Switch (PRIMEQUEST 520A/520/420) (→ 3.3.5)
- High Reliability Tools (→ 3.3.6)

Hinweis: Verwenden Sie zur Installation von Windows Server 2003, Enterprise Edition (IA64), das Sie mit einer Volume License gekauft haben, SystemcastWizard Lite.

3.3.1 Installationsvorbereitungen

In diesem Handbuch werden nur die für die Installation der PRIMEQUEST erforderlichen Schritte beschrieben. Eine Beschreibung der zur Konfiguration und Feinabstimmung der SAN-Speicherprodukte und der Fibre Channel Switches erforderlichen Verfahren finden Sie in den entsprechenden Handbüchern. Die SAN Boot Environment wird von einem Kundendienst-Techniker eingerichtet. Wenden Sie sich für weitere Informationen an Ihren zuständigen Techniker.

3.3.1.1 SAN Boot Environment einrichten

Folgende Aufgaben sind zur Einrichtung der SAN Boot Environment erforderlich. Weitere Einzelheiten finden Sie in Anhang D, „SAN Boot Environment“.

- SAN Boot Environment konzipieren
  Der Grad an Verfügbarkeit, der erlangt werden kann, hängt zu einem großen Teil von der Topologie der PRIMEQUEST, des SANs und der Fibre Channel Switches ab.
- SAN-Booteinstellungen für die PRIMEQUEST festlegen
  Richten Sie die SAN-Speichereinheiten und die PRIMEQUEST gemäß dem Konfigurationsplan ein. Der EFI-Treiber des Fibre Channel muss konfiguriert sein.
- SAN-Speicher und Fibre Channel Switches einrichten
  SAN-Speichereinheiten und Fibre Channel Switches gemäß dem Verbindungsplan installieren, anschließen, konfigurieren und feinabstimmen.

3.3.1.2 SAN-Speichereinheit anschließen

Um das Betriebssystem auf einem SAN-Speicher zu installieren, muss eine SAN-Speichereinheit wie in Abschnitt 3.3.1.1 beschrieben vorbereitet werden. Die in Abschnitt 3.3.2 und 3.3.4 beschriebenen Installationsverfahren gehen davon aus, dass die folgenden Schritte durchgeführt wurden:

Um Windows auf einem SAN-Speicher zu installieren, müssen zusätzlich die folgenden Bedingungen erfüllt sein. Überprüfen Sie nach der Installation, dass Windows starten kann, und konfigurieren Sie es für die Einsatzumgebung.

- Nur die LUNs, auf denen Windows installiert ist, können von der PRIMEQUEST aus angesprochen werden.
- Die PRIMEQUEST ist mit dem SAN-Speicher nur über einen einzigen Pfad verbunden.

Windows mit SystemcastWizard Lite auf einem SAN-Speicher installieren

- Installationsserver
- Konsole (Tastatur, Bildschirm, Maus)
- Externes RAID (z.B. ETERNUS*)
- Fibre Channel-Karte
- LWL-Kabel
- LAN-Kabel

Windows mit KVM auf einem SAN-Speicher installieren

- Konsole (Tastatur, Bildschirm, Maus)
- Externes RAID (z.B. ETERNUS*)
- Fibre Channel-Karte
- LWL-Kabel
- Diskettenlaufwerk (muss separat vorbereitet werden)

Ferner müssen die unten genannten Bedingungen erfüllt sein, damit Windows auf dem SAN-Speicher installiert werden kann. Wenn die Installation von Windows abgeschlossen ist, überprüfen Sie, ob Windows normal gestartet ist, und ändern Sie erforderlichenfalls die Betriebskonfiguration.

- Die PRIMEQUEST erkennt nur das LUN, das das Ziel der Windows-Installation ist.
- Die PRIMEQUEST und der SAN-Speicher sind über einen einfachen Pfad verbunden.

*: Angebot und Support in EMEA nur für die globalen Kunden von Fujitsu

3.3.1.3 Vor der Installation (PRIMEQUEST 580A/540A*/580/540/480/440)

Hinweis: Windows unterstützt nicht den PCI Segment Mode. Stellen Sie mithilfe der MMB Web-UI wie im Folgenden beschrieben den PCI Bus Mode ein, wenn Sie mit PRIMEQUEST Partitionen einrichten.

Gehen Sie wie folgt vor, um den PCI Bus Mode einzustellen:

1 Wählen Sie in der MMB Web-UI [Partition] → [Partition#x] → [Mode] aus. Das Fenster [Mode] wird angezeigt.

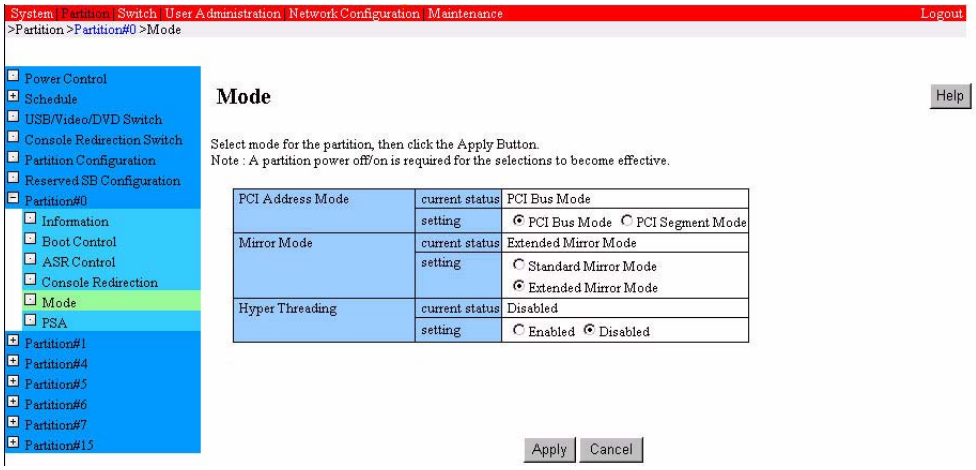


Abbildung 3.14 Das Fenster [Mode] (PRIMEQUEST 580A/540A*)

2 Wählen Sie die Option [PCI Bus Mode] aus und klicken Sie auf [Apply], um die Einstellung zu bestätigen.
Es erscheint die Meldung „A Partition power off/on is required in order to make set...“. Klicken Sie auf [OK], um fortzufahren.

Hinweis: Installieren Sie Windows, wenn die Plattenpartition sich im geeigneten Zustand befindet. Wenn Sie die Installation im Overwrite-Modus durchführen und Linux bereits installiert ist, schlägt der Versuch fehl. Initialisieren Sie die Platte, bevor Sie Windows in einer solchen Umgebung installieren. Einzelheiten zur Initialisierung einer SAN-Platte finden Sie in Handbuch der SAN-Speichereinheit beschrieben.

*: wird von Fujitsu Technology Solutions nicht unterstützt

3.3.2 Windows mit SystemcastWizard Lite installieren

3.3.2.1 Hardwarevoraussetzungen und Vorgehensweise

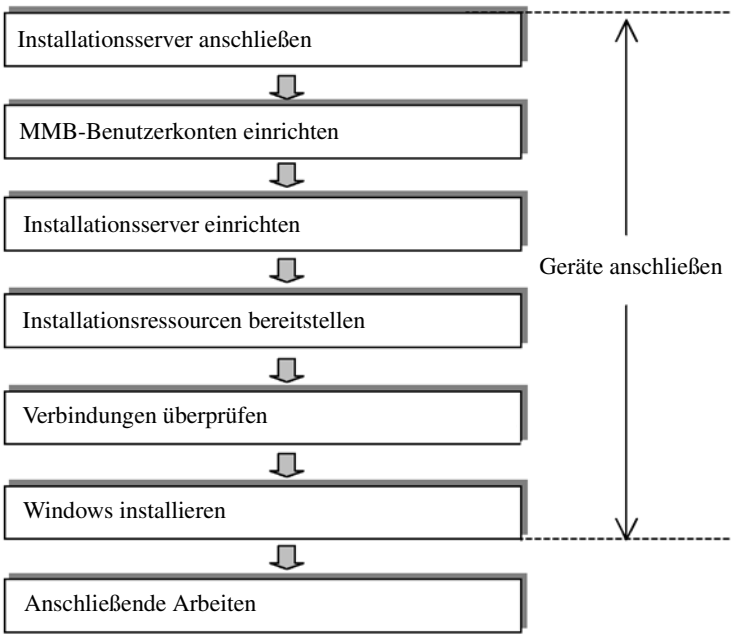
Bevor Sie das Betriebssystem mit SystemcastWizard Lite installieren können, müssen Sie einen PC entsprechend vorbereiten. Installieren Sie SystemcastWizard Lite auf einem PC und benutzen Sie diesen als Installationsserver, auf dem die erforderlichen registrierten Ressourcen und Informationen gespeichert werden können.

Tabelle 3.7 enthält einen Überblick über die Systemvoraussetzungen. Weiteres finden Sie im *PRIMEQUEST SystemcastWizard Lite User's Guide* (C122-E010EN).

Tabelle 3.7 Systemvoraussetzungen im Überblick

Komponente	Voraussetzugen
Hardware	PRIMERGY/FMV Serie (IA-32) Ein DVD-ROM-Laufwerk ist erforderlich, um die Windows Server 2003 (IA64) Installations-DVD zu lesen. Eines der folgenden Betriebssysteme ist erforderlich: • Windows Server 2003, Standard Edition (Service Pack 1 oder höher) • Windows Server 2003, Enterprise Edition (Service Pack 1 oder höher) • Windows Server 2003 R2, Standard Edition • Windows Server 2003 R2, Enterprise Edition • Windows XP Professional (Service Pack 2 oder höher) • Windows Vista Business • Windows Vista Enterprise
	LAN-Kabel
Software	SystemcastWizard Lite, PRIMEQUEST Software-Bundle-Package

Die Installation umfasst folgende Schritte:



3.3.2.2 Geräte anschließen

Gehen Sie wie folgt vor, um die Geräte anzuschließen:

(1) Installationsserver

1 Schließen Sie den Installationsserver am Netzwerk an.
Einzelheiten über die Installation von SystemcastWizard Lite finden Sie im *PRIMEQUEST SystemcastWizard Lite User's Guide* (C122-E010EN).

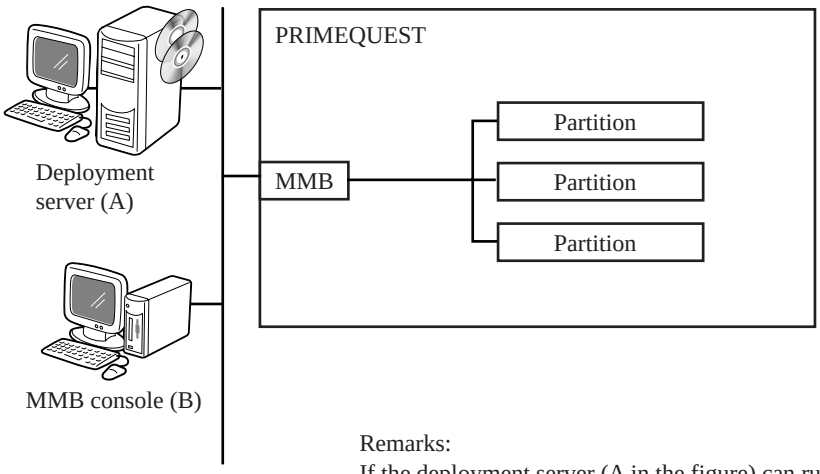

PRIMEQUEST
Partition
Partition
Partition
MMB
Deployment server (A)
MMB console (B)
Management LAN
Remarks:
If the deployment server (A in the figure) can run the Web browser, the deployment server can be used as the MMB console. In such case, you do not need to obtain a separate MMB console (B in the figure).

Abbildung 3.15 Anforderungen für die Installation mit SystemcastWizard Lite (Windows)

Hinweis: Obwohl das Netzwerk mit PXE aktiviert ist, können Sie es nicht über einen Router aktivieren. Schließen Sie den Installationsserver daher an das Management-LAN an, an das auch die PRIMEQUEST angeschlossen ist.

Die Zielpartition wird entfernt gestartet oder das MMB 0 wird für die gesamte Kommunikation für Datensicherungen und -wiederherstellungen benutzt. Dazu sollten Sie das MMB 0 immer an das Management-LAN angeschlossen haben, es muss allerdings nicht aktiv sein.

(2) Benutzerkonten für den Zugriff auf das MMB einrichten

Sie können die für die entfernte Steuerung des MMB mit SystemcastWizard Lite erforderlichen Benutzerdaten festlegen.

Wenn Sie dazu aufgefordert werden, schließen Sie das USB-Diskettenlaufwerk an den USB-Port der KVM-Einheit an und legen Sie die vorbereitete Diskette mit den Treibern ein.

1 Wählen Sie [Network Configuration] → [Remote Server Management] im MMB Web-UI. Das Fenster [Remote Server Management] wird angezeigt.

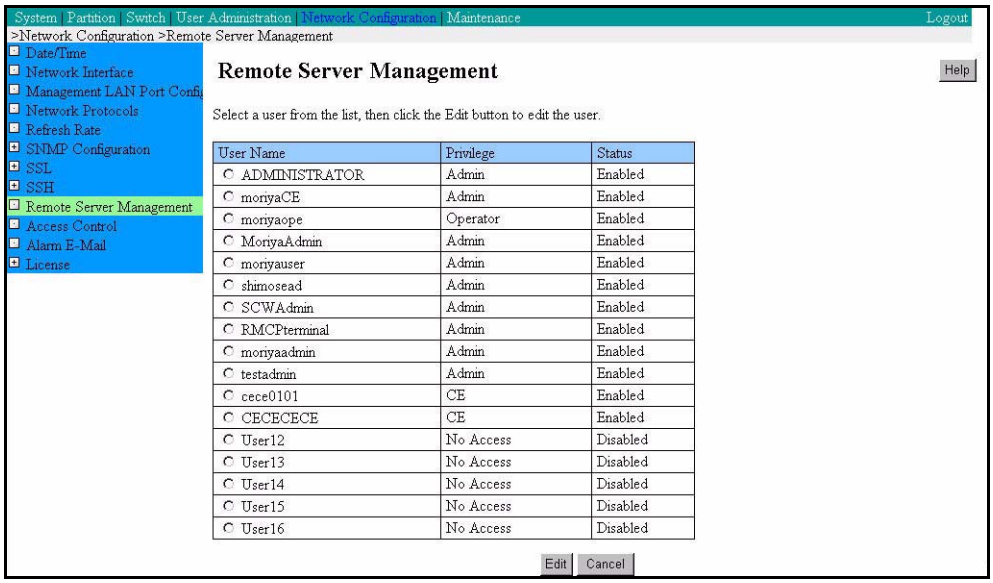


Abbildung 3.16 Das Fenster [Remote Server Management]

2 Wählen Sie den betreffenden Benutzer aus, indem Sie das dazugehörige Optionsfeld anklicken und klicken Sie dann auf die Schaltfläche [Edit].
Das Fenster [Edit User] wird angezeigt.

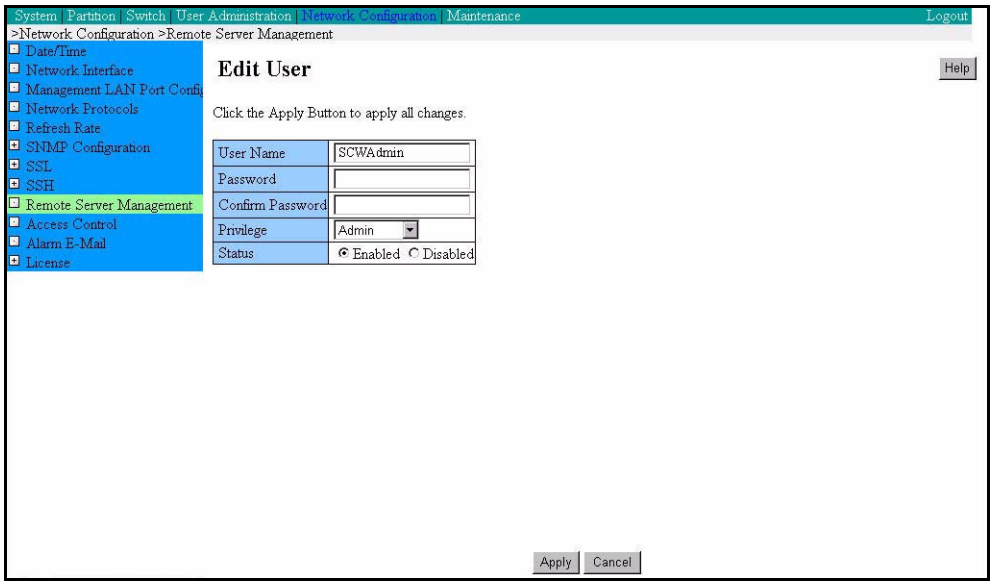


Abbildung 3.17 Das Fenster [Edit User]

3 Geben Sie im Fenster [Edit User] die Benutzerverwaltungsdaten ein und klicken Sie auf [Apply], um die Eingaben zu bestätigen.
- User Name: Geben Sie einen Benutzernamen ein (8 bis 16 Zeichen).
- Password: Geben Sie ein Kennwort ein (8 bis 16 Zeichen).
- Confirm Password: Wiederholen Sie das Kennwort zur Bestätigung.
- Privilege: Wählen Sie aus der Dropdown-Liste Admin aus.
- Status: Wählen Sie die Option Enabled.

(3) Installationsserver einrichten

1 Registrieren Sie die Partition, auf der Sie Linux installieren wollen, auf dem Installationsserver. Benutzen Sie dazu die graphische Bedienoberfläche (Installationskonsole) des SystemcastWizard Lite. Einzelheiten finden Sie im *PRIMEQUEST SystemcastWizard Lite User's Guide* (C122-E010EN).

(4) Ressourcen für die Installation bereitstellen

Eine genaue Beschreibung der für die Installation mit SystemcastWizard Lite erforderlichen Ressourcen finden Sie im *PRIMEQUEST SystemcastWizard Lite User's Guide* (C122-E010EN).

3.3.2.3 Windows installieren

Legen Sie auf der Installationskonsole die Ressourcen an und installieren Sie Windows.
Einzelheiten finden Sie im *PRIMEQUEST SystemcastWizard Lite User's Guide* (C122-E010EN).

Anm.:

- Wenn das Betriebssystem vollständig installiert ist, führen Sie die im Abschnitt 3.1.4, „Nach Installation des Betriebssystems erforderliche Arbeiten“ beschriebenen Schritte durch.
- Die High Reliability Tools können mit SystemcastWizard Lite zusammen mit dem Betriebssystem installiert werden. Näheres finden Sie im *PRIMEQUEST SystemcastWizard Lite User's Guide* (C122-E010EN).
- Die benötigten Produktkennungen finden Sie in Tabelle 3.9.

3.3.3 Installation von Windows mit dem Installation Support Tool

3.3.3.1 Übersicht

Das Installation Support Tool für Windows ist ein Tool zur automatisierten Windows-Installation, das zusammen mit der PRIMEQUEST ausgeliefert wird.

Das Installation Support Tool für Windows macht es erforderlich, dass die Installationsparameter zuvor auf einem (32-bit) Computer unter Windows erfasst und auf einer Diskette gespeichert werden. Diese Diskette wird „installation floppy disk“ genannt.

Unter Verwendung dieser Installationsdiskette ermöglicht das Installation Support Tool für Windows die automatisierte Installation auf einer PRIMEQUEST von der Installations-DVD. Im Anschluss an die Installation installiert der PRIMEQUEST Software Installer Treiber und Überwachungs-Tools, die für einen stabilen Systembetrieb erforderlich sind.

Die Installation unter Verwendung des Installation Support Tool für Windows hat folgende Vorteile:

- Die Verwendung einer Installationsdiskette, die vorher überprüft wurde, kann Verfahrensfehler während der Installation verhindern.
- Vorgänge, um Windows in vielen Partitionen mit derselben Konfiguration zu installieren, können leicht durchgeführt werden.

- Verglichen mit der Installation mithilfe von SystemcastWizard Lite, ist die Bedienung der Geräte einfach, da eine einzige Diskette die notwendigen Daten enthält. Nur ein USB-Diskettenlaufwerk ist für die Installation erforderlich.

Das Installation Support Tool für Windows findet sich unter folgendem Pfad auf der „PRIMEQUEST Drivers CD for Microsoft® Windows Server® 2003“ (C122-E024) (die in diesem Dokument Treiber-CD genannt wird), die mit der PRIMEQUEST geliefert wird:

E:\Tools\General\IST (wobei das CD-ROM-Laufwerk hier Laufwerk E ist)

Einzelheiten finden Sie in der Readme-Datei und im *PRIMEQUEST Installation Support Tool for Windows User's Guide* (C122-048EN).

3.3.3.2 Vorbereitungen

Um das Installation Support Tool für Windows für die Windows-Installation auf der PRIMEQUEST verwenden zu können, müssen zuvor folgende Vorbedingungen erfüllt sein.

- Konsolbildschirm/Tastatur/Maus
  eines Terminals, das an die PRIMEQUEST angeschlossen ist
- Ein USB-Disketten-Laufwerk,
  das an die PRIMEQUEST angeschlossen ist
- Ein Computer mit Windows XP oder Windows 2000
  Das Installation Support Tool für Windows läuft auf diesem PC ab. Tabelle 3.8 enthält die Systemanforderungen.
- Windows Installations-DVD
  Windows Server 2003 for Itanium DVD. Die Version auf dieser DVD beinhaltet bereits Service Pack 1.
- Treiber-CD
  CD-ROM, die das Installation Support Tool for Windows enthält.
- 1.44-MB-Diskette
  Formatieren Sie zuvor die Diskette mit Windows.

Tabelle 3.8 Systemvoraussetzungen für das Installation Support Tool for Windows

Anforderung	kompatibilität
Betriebssystem	Japanische oder englische Version eines der folgenden Betriebssysteme: • Windows® Vista Enterprise • Windows® Vista Business • Windows® XP Professional (mit Service Pack 2 oder höher) • Windows® XP Home Edition (mit Service Pack 2 oder höher) • Windows® 2000 Professional (mit Service Pack 4 oder höher)
CPU	32-bit-CPU Eine solche CPU erfüllt die Anforderungen der Betriebssysteme.
Hauptspeicher	Der Hauptspeicher muss die Anforderungen der Betriebssysteme erfüllen.
Festplattenspeicher	Freier Plattenplatz für mindestens 1 MB für temporäre Verzeichnisse muss vorhanden sein.
Sonstiges	Es werden ein CD-ROM-Laufwerk und ein Disketten-Laufwerk benötigt.

Hinweis: Einschränkungen bei der Installation von Windows Server 2003, Enterprise Edition
Das Installation Support Tool for Windows kann nicht zur Installation von Windows Server 2003, Enterprise Edition (IA64) verwendet werden, wenn es mit einer Volume License gekauft wurde. Benutzen Sie in diesem Fall SystemcastWizard Lite, das mit dem PRIMEQUEST-Produkt ausgeliefert wird.

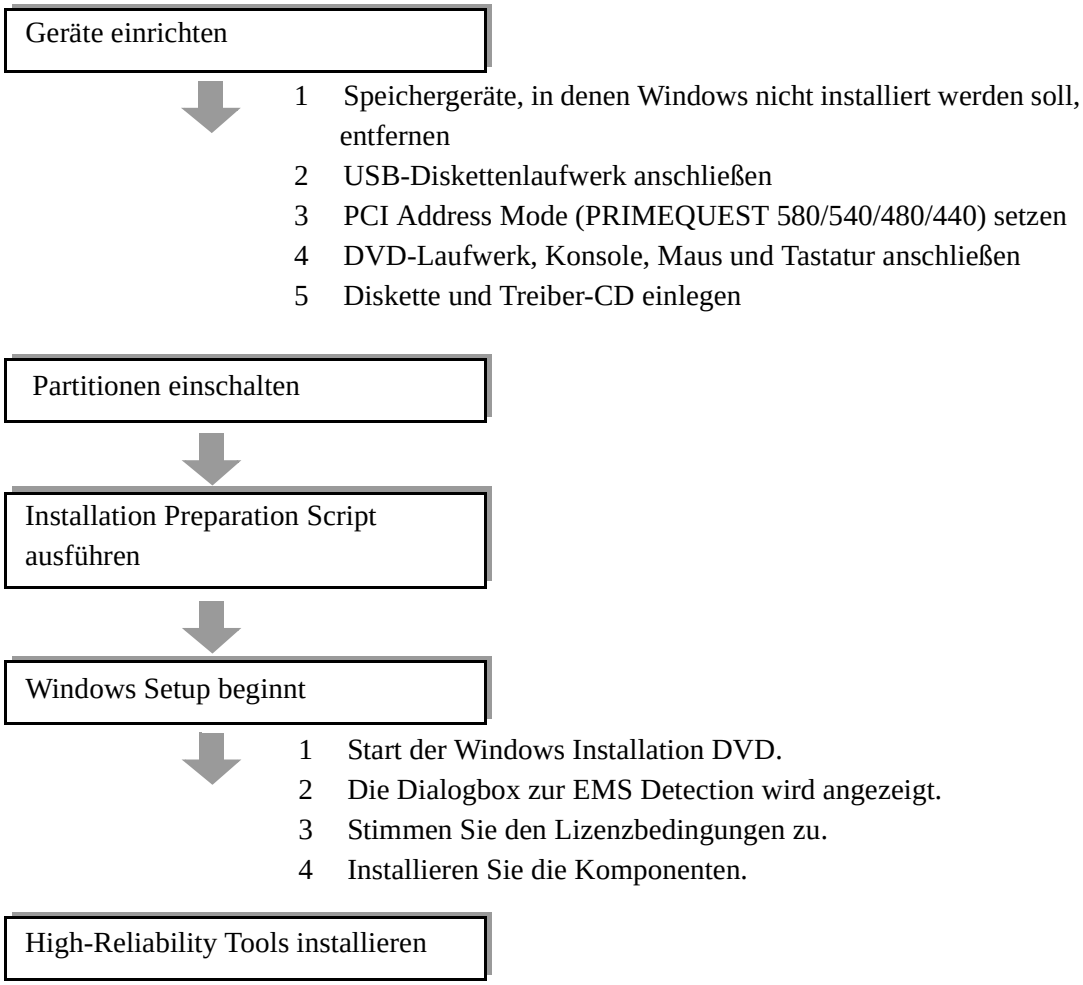
3.3.3.3 Erstellen der Installationsdiskette

Starten Sie das Installation Support Tool for Windows. Legen Sie die CD in den vorbereiteten PC, und rufen Sie vom Explorer folgendes Programm auf:

E:\Tools\General\IST\ISTWin.exe
(wenn das CD-ROM-Laufwerk E ist)

3.3.3.4 Windows-Setup

Der Ablauf ist folgendermaßen:


Geräte einrichten
1 Speichergeräte, in denen Windows nicht installiert werden soll, entfernen
2 USB-Diskettenlaufwerk anschließen
3 PCI Address Mode (PRIMEQUEST 580/540/480/440) setzen
4 DVD-Laufwerk, Konsole, Maus und Tastatur anschließen
5 Diskette und Treiber-CD einlegen
Partitionen einschalten
Installation Preparation Script ausführen
Windows Setup beginnt
1 Start der Windows Installation DVD.
2 Die Dialogbox zur EMS Detection wird angezeigt.
3 Stimmen Sie den Lizenzbedingungen zu.
4 Installieren Sie die Komponenten.
High-Reliability Tools installieren

Einzelheiten finden Sie im *PRIMEQUEST Installation Support Tool for Windows User's Guide* (C122-048EN).

3.3.4 Installation von Windows mit KVM (PRIMEQUEST 580A/540A*/ 580/540/480/440)

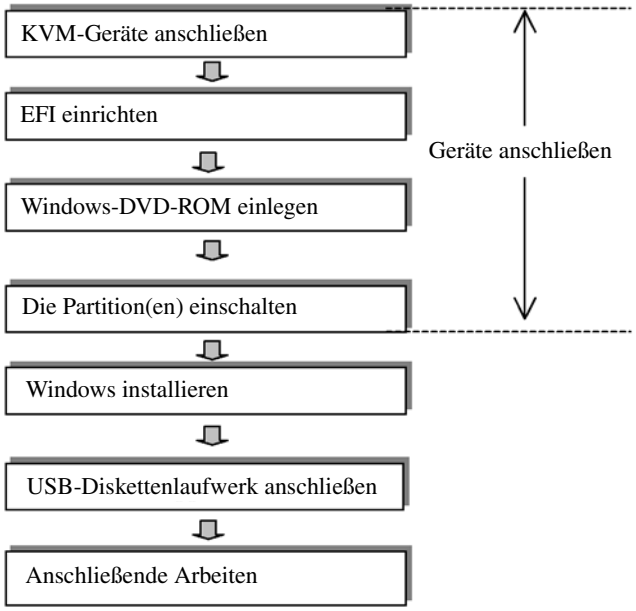
3.3.4.1 Hardwarevoraussetzungen und Verfahren

Die folgenden Geräte müssen angeschlossen sein, damit Sie Windows mithilfe der KVM-Einheit auf einem SAN-Laufwerk installiert werden kann:

- Tastatur
- Bildschirm
- Maus
- SAN-Speichereinheit (z.B. ETERNUS**)
- Fibre Channel-Karte
- LWL-Kabel
- Diskettenlaufwerk
  (muss separat vorbereitet werden. Wird während der Windows-Installation angeschlossen).

Anm.: Einzelheiten über den Anschluss der ETERNUS**-Einheiten an die PRIMEQUEST finden Sie im Handbuch des SAN-Speichers.

Die Installation umfasst folgende Schritte:



*: wird von Fujitsu Technology Solutions nicht unterstützt
**: Angebot und Support in EMEA nur für die globalen Kunden von Fujitsu

3.3.4.2 Geräte anschließen

Gehen Sie wie folgt vor, um die KVM-Einheit an die Partition anzuschließen, auf der Sie Windows installieren wollen:

(1) KVM-Einheit anschließen

1 Schließen Sie eine Tastatur, eine Maus und einen Bildschirm an die KVM-Einheit an.

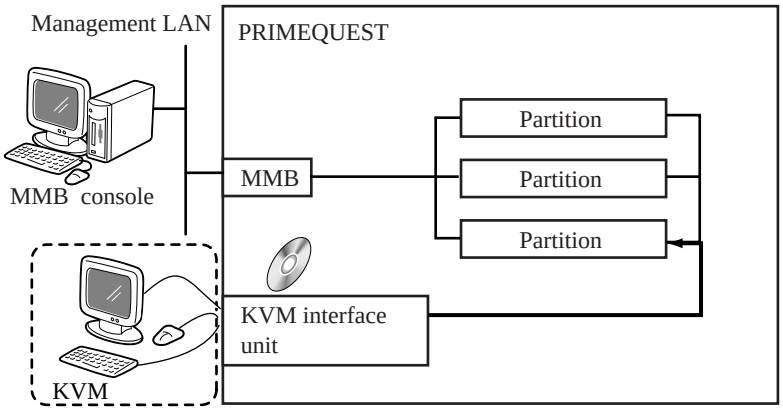


Abbildung 3.18 Anschlüsse für eine Installation mit KVM

2 Wählen Sie in der MMB Web-UI [Partition] → [USB/Video/DVD Switch]. Das Fenster [USB/Video/DVD Switch] wird angezeigt.

Anm.: Im 2.2.2.1, „An- und Abmelden bei der MMB Web-UI“ wird beschrieben, wie Sie sich beim MMB Web-UI anmelden.

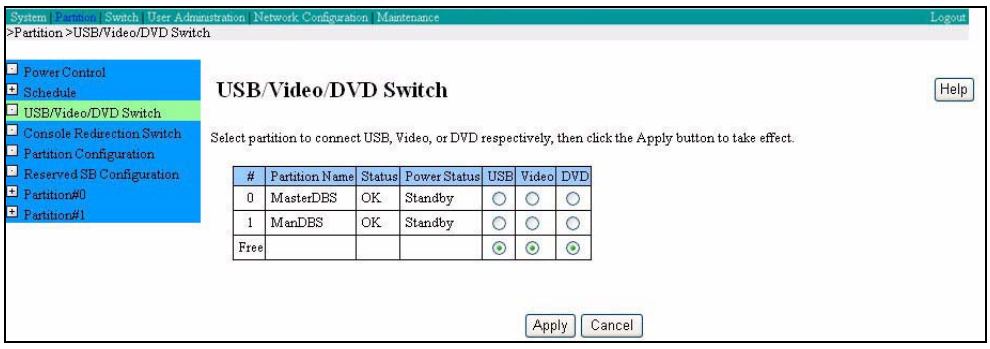


Abbildung 3.19 Das Fenster [USB/Video/DVD Switch]

3 Aktivieren Sie die Optionsfelder in den Spalten USB, Video und DVD der Partition, auf der Sie das Betriebssystem installieren wollen und klicken Sie dann auf [Apply], um die Auswahl zu bestätigen.

3.3.4.3 Windows installieren

Dieser Abschnitt beschreibt, wie Sie Windows auf einem SAN-Laufwerk oder einem internen Laufwerk installieren.

1 Legen Sie die DVD-ROM mit Windows Server 2003 in das DVD-ROM-Laufwerk der KVM-Einheit ein.

2 Wählen Sie im MMB Web-UI [Partition] → [Power Control].
Das Fenster [Power Control] wird angezeigt.

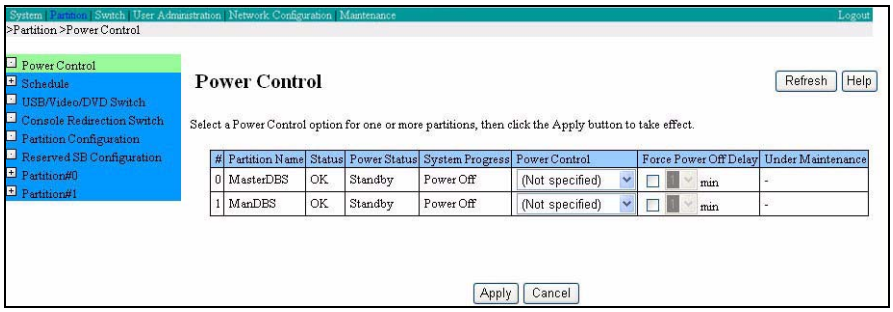

System | Partition | Switch | User Administration | Network Configuration | Maintenance
Logout
>Partition >Power Control
Power Control
Schedule
USB/Video/DVD Switch
Console Redirection Switch
Partition Configuration
Reserved SB Configuration
Partition#0
Partition#1
Power Control
Refresh
Help
Select a Power Control option for one or more partitions, then click the Apply button to take effect.
| Partition Name | Status | Power Status | System Progress | Power Control | Force Power Off Delay | Under Maintenance
0 | MasterDBS | OK | Standby | Power Off | (Not specified) | min | -
1 | ManDBS | OK | Standby | Power Off | (Not specified) | min | -
Apply
Cancel

Abbildung 3.20 Fenster [Power Control]

3 Wählen Sie in der Spalte [Power Control] der Partition, auf der Sie Windows installieren wollen, aus der Dropdown-Liste [Power On], um sie einzuschalten.
Anm.: Wenn die Partition bereits eingeschaltet ist, wählen Sie [Reset].

- Installation auf einer SAN-Speichereinheit, z.B. ETERNUS*
  Benutzen Sie den Fibre Channel-Kartentreiber (FC Driver), den Sie auf der CD „PRIMEQUEST Drivers CD for Microsoft® Windows Server® 2003“ (C122-E024) finden (in diesem Handbuch Treiber-CD genannt).
  Bereiten Sie die Treiber-Diskette auf einem separaten Windows-PC vor.
- Treiber-Diskette für Fibre Channel vorbereiten
  1 Formatieren Sie eine Diskette.
  2 Legen Sie die Treiber-CD in das CD-Laufwerk eines separaten PCs.
  3 Öffnen Sie in einem Explorer-Fenster den folgenden Ordner auf der Treiber-CD:
  E:\Drivers\FC\Emulex (wenn E das CD-ROM-Laufwerk ist)
  4 Markieren Sie alle Dateien im Ordner und kopieren Sie sie auf die Diskette.

Installation auf einem internen Laufwerk
Benutzen Sie den SCSI-Treiber, den Sie auf der „PRIMEQUEST Drivers CD for Microsoft® Windows Server® 2003“ (C122-E024) finden (in diesem Handbuch Treiber-CD genannt).

*: Angebot und Support in EMEA nur für die globalen Kunden von Fujitsu

- Treiber-Diskette für SCSI vorbereiten
  1 Formatieren Sie eine Diskette.
  2 Legen Sie die Treiber-CD in das CD-Laufwerk eines separaten PCs.
  3 Öffnen Sie in einem Explorer-Fenster den folgenden Ordner auf der Treiber-CD:
  E:\Drivers\SCSI\LSILogic (wenn E das CD-ROM-Laufwerk ist)
  4 Markieren Sie alle Dateien im Ordner und kopieren Sie sie auf die Diskette.

4 Klicken Sie auf [Apply], um die Einstellung zu bestätigen.
Die Meldung [EFI Boot Manager] wird auf der Konsole angezeigt, die mit dem KVM-Gerät verbunden ist.

```
EFI Boot Manager  ver 1.xx [xx.xx]

Please Select a boot option
DVD /Acpi(xxxxxxxx)
Network Boot/Pci(1|0|0)/Mac(0007E9D80F36)
EFI Shell [Built in]
Boot option maintenance menu
```

Hinweis: Stellen Sie sicher, dass das USB Diskettenlaufwerk nicht installiert ist.
Wird eine Diskette in ein USB-Laufwerk eingelegt, kann folgende Meldung erscheinen:

```
INF file txtsetup is corrupt or missing,status 18.
Setup cannot continue. Press any key to exit.
```

In diesem Fall drücken Sie [Enter], um Windows neu zu starten, und ziehen Sie den Anschluss des USB-Diskettenlaufwerks heraus und stecken Sie ihn dann wieder ein. Fahren Sie daraufhin mit Schritt 4 fort.
Wenn Windows nicht neu startet, nachdem Sie die [Enter]-Taste gedrückt haben, ziehen Sie den Anschluss des USB-Diskettenlaufwerks heraus, stecken Sie ihn dann wieder ein und fahren Sie mit Schritt 2 fort.
Schließen Sie das USB-Diskettenlaufwerk an den PC an, wenn Sie die Treiber manuell installieren.

5 Wählen Sie „DVD /Acpi (xxxxxxxx)“ und drücken Sie die [Enter]-Taste.
Wenn der Festplatte ein aktiver Bereich zugewiesen wurde, erscheint die folgende Meldung. Drücken Sie, während diese Meldung angezeigt wird, eine beliebige Taste, um das System vom DVD-ROM-Laufwerk aus zu laden.

```
Press any key to boot from CD ... .
```

6 Der Installationsbildschirm von Windows Server 2003 wird angezeigt.
Unten auf dem Installationsbildschirm erscheint sofort nach dessen Anzeige die folgende Meldung.
Diese Meldung wird für kurze Zeit unmittelbar nach dem Setup Screen (blue screen) angezeigt. Drücken Sie sofort die [F6]-Taste, nachdem der Setup Screen (blue screen) angezeigt wurde.

```
Press F6 if you need to install third party
SCSI or RAID driver ... .
```

7 Installieren Sie den Treiber manuell.

1 Drücken Sie die [S]-Taste, wenn die folgende Meldung erscheint:

```
To specify additional SCSI adapters, CD-ROM drivers,
or special disk controllers for use with Windows,
including those for which you have a device support
disk from mass storage device manufacturer, press S
```

2 Wenn die folgende Meldung erscheint, schließen Sie das USB-Diskettenlaufwerk an den USB-Port der KVM-Einheit an und legen Sie die in Schritt 3 vorbereitete Treiberdiskette ein.

```
Please insert disk labeled Manufacture-supplied hard-
ware support disk into Drive A:
```

3 Drücken Sie die [Enter]-Taste. Die folgende Meldung erscheint:

```
You have chosen to configure a SCSI adapter for use
with Windows, using a device support disk provided by
an adapter manufacturer. Select the SCSI adapter you
want from the following list, or press ESC to return
the previous screen
```

4 Wählen Sie die folgende Option aus und drücken Sie die [Enter]-Taste:

```
Emulex LPX000 PCI Fibre Channel HBA
```

Wählen Sie für SCSI die folgende Option aus:

```
LSI Logic PCI Fusion-MPT Driver (Server 2003 IA64)
```

Folgen Sie den auf dem Bildschirm angezeigten Anweisungen, um die Fibre Channel-Treiber für möglicherweise in einer Partition installierte Fibre Channel-Karten zu installieren, selbst wenn deren Kabel nicht angeschlossen ist.

Hinweis: Entfernen Sie das Disketten-Laufwerk nicht, bevor die Installation beendet ist.

8 Fahren Sie mit der Installation fort, indem Sie den Anweisungen des Installationsprogramms folgen.
Weitere Einzelheiten finden Sie im Handbuch des Betriebssystems.
Wird in einer Meldung im Verlauf der Installation eine Diskette verlangt, dann legen Sie die Treiber-Diskette ein und drücken Sie die [Enter]-Taste.
Anm.: Während der Installation wird die Produktkennung angefordert. Je nach Betriebssystem und Kaufverfahren finden Sie diese an einer anderen Stelle.

Tabelle 3.9 Produktkennungen

Betriebssystem	Kaufverfahren	Produktkennung
Windows Server 2003, Enterprise Edition für Itanium-basierte Systeme	Datenträger-Lizenz	CD-Paket mit den Medien für das Betriebssystem
	zusammen mit der Hardware	CoA-Etikett auf der Systemeinheit oder einer separaten Einheit (*1)(*2)(*3)
Windows Server 2003, Datacenter Edition für Itanium-basierte Systeme	zusammen mit der Hardware	CoA-Etikett auf der Systemeinheit oder einer separaten Einheit (*1)(*2)(*4)

*1:Lesen Sie die „Important Notice“ der Systemeinheit, um zu erfahren, wo sich das CoA-Etikett mit der Produktkennung befindet.
*2:Wenn das CoA-Etikett eine separate Einheit ist, lesen Sie unbedingt die „Important Notice“, die zu deren Lieferumfang gehört, und bringen Sie das Etikett dann auf der Systemeinheit an.
*3:Verwenden Sie ein CoA-Etikett, das mit „Enterprise“ gekennzeichnet ist. Gibt es mehrere CoA-Etikette mit dieser Kennzeichnung, müssen Sie darauf achten, dass Sie während der Installation ausschließlich eine Produktkennung verwenden.
*4:Verwenden Sie ein CoA-Etikett für Datacenter, das mit „4 CPU“ gekennzeichnet ist.

9 Starten Sie das System neu. Im Bildschirm des EFI Boot Manager wurde „Windows Server 2003, Datacenter“ oder „Windows Server 2003, Enterprise Edition“ hinzugefügt. Wählen Sie diese Option des Boot-Menüs aus, um Windows zu starten.

10 Installieren Sie die Tools zur Erhöhung der Betriebszuverlässigkeit (High-Reliability Tools), nachdem Windows gestartet ist. Einzelheiten finden Sie in 3.3.6.1, „Installation mit PRIMEQUEST Software Installer“.

3.3.4.4 Bedienerlose Installation

Mit dem Emergency Management Service (EMS) von Windows Server 2003 ist eine bedienerlose Installation über KVM möglich. Sie brauchen hierzu ein COM-Kabel und einen Notebook-PC mit COM-Port.

Stellen sie sicher, dass im Fenster [Console Redirection Switch] in der Auswahl [Partition] im MMB Web-UI „COM“ als Partition, auf der Sie Windows installieren wollen, angegeben ist.

Hinweise zur bedienerlosen Installation

- Das COM-Kabel muss an den COM-Port der IO Unit angeschlossen werden.
- Tastatureingaben für die Terminalsoftware weichen von jenen für die Bildschirmeingabe ab.
  Wenn das Installationsprogramm Sie beispielsweise auffordert, eine Funktionstaste [Fx] zu drücken, drücken Sie die [ESC]-Taste und dann die Taste mit der Ziffer „x“.
  Wenn das Installationsprogramm Sie auffordert, die [Bild nach unten]-Taste zu drücken, drücken Sie die [ESC]-Taste und dann die [/]-Taste.
  Wenn das Installationsprogramm Sie auffordert, die [Bild nach oben]-Taste zu drücken, drücken Sie die [ESC]-Taste und dann die [?]-Taste.

  Hinweis: Drücken Sie die Zifferntaste, [/]-Taste bzw. [?]-Taste sofort nach der [ESC]-Taste. Wenn der zeitliche Abstand zwischen der Betätigung der [ESC]-Taste und der zweiten Taste zu lang ist, erkennt das System eventuell nur die [ESC]-Taste und interpretiert den Tastendruck als Befehl zum Neustart.

- Wählen Sie den Tastaturtyp wie folgt aus:

1 Drücken Sie die [s]-Taste, wenn der Auswahlbildschirm für den Tastaturtyp angezeigt wird.

```
Press one of the following keys to select a keyboard
type:

en-size/em-size key: 106 Japanese keyboard
Space key: 101 English keyboard
"S" key: Other keyboard

-  To quit setup, press the [F3] key.
```

2 Mit 101 wählen Sie die englische Tastatur aus.

```
Select a keyboard type from the following list:

-  To continue setup, press the [Enter] key.
-  To quit setup, press the [F3] key.

  +-------------------------------------------------+
  | 106 Japanese Keyboard (Including USB)           |
  | 101 English Keyboard (Including USB)            |
  | NEC 98 Layout USB Keyboard                      |
  | USB Keyboard                                    |
  +------------------------------(Scroll down  )--+
```

- Verwenden Sie eine Terminalanschluss-Software, die UTF-8 unterstützt.
  Eine Terminalanschluss-Software, die UTF-8 nicht unterstützt, zeigt Zeichen möglicherweise fehlerhaft an.

Installation

Verwenden Sie eine Terminalanschluss-Software, um eine Verbindung herzustellen. Als Standardsoftware wird mit Windows XP HyperTerminal bereitgestellt. Das Beispiel in diesem Abschnitt verwendet Tera Term.

Stellen Sie eine Datenübertragungssoftware wie folgt ein:

Tabelle 3.10 Terminalsoftware-Einstellungen

Parameter	Wert
Bits/second	19200
Data bits	8
Parity	None
Stop bit	1
Flow control	None
Emulation	VT100

Bereiten Sie Treiber-Disketten gemäß Schritt 3 in 3.3.4.3, „Windows installieren“ vor. Wenn die Anzeigen auf dem blauen Bildschirm komplett ist, nehmen Sie die im Folgenden beschriebenen Einstellungen vor.

1 Starten Sie Tera Term. Drücken Sie die [ESC]- und die [TAB]-Taste, wenn der folgende Bildschirm erscheint.

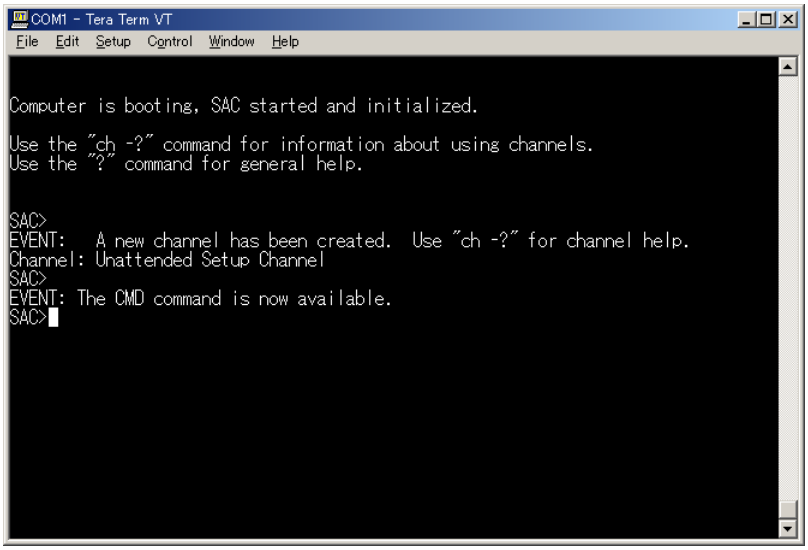

COM1 - Tera Term VT
File Edit Setup Control Window Help
Computer is booting, SAC started and initialized.
Use the "ch -?" command for information about using channels.
Use the "?" command for general help.
SAC>
EVENT: A new channel has been created. Use "ch -?" for channel help.
Channel: Unattended Setup Channel
SAC>
EVENT: The CMD command is now available.
SAC>

Abbildung 3.21 Tera Term-Startfenster

2 Drücken Sie die [Enter]-Taste, wenn der folgende Bildschirm erscheint.

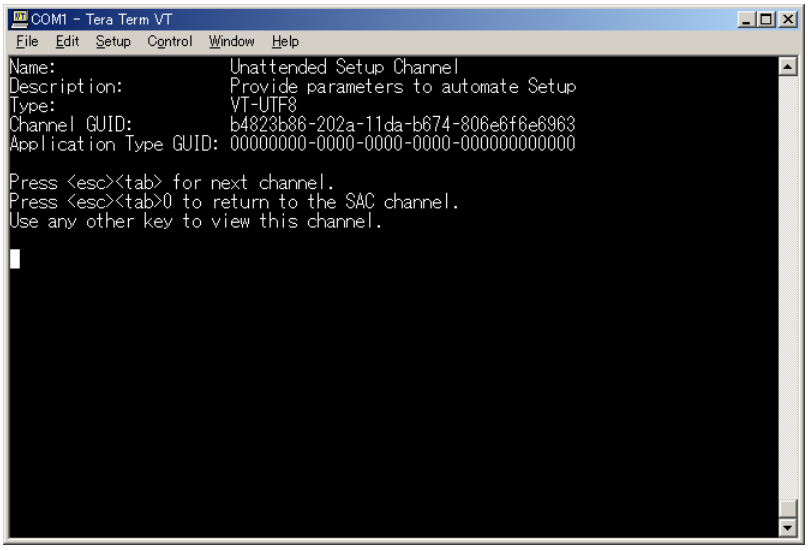

COM1 - Tera Term VT
File Edit Setup Control Window Help
Name: Unattended Setup Channel
Description: Provide parameters to automate Setup
Type: VT-UTF8
Channel GUID: b4823b86-202a-11da-b674-806e6f6e6963
Application Type GUID: 00000000-0000-0000-0000-000000000000
Press <esc><tab> for next channel.
Press <esc><tab>0 to return to the SAC channel.
Use any other key to view this channel.

Abbildung 3.22 Setup-Fenster

3 Wenn der folgende Bildschirm erscheint: Bestätigen Sie, Drücken Sie die [ESC]-Taste und dann die [8]-Taste.

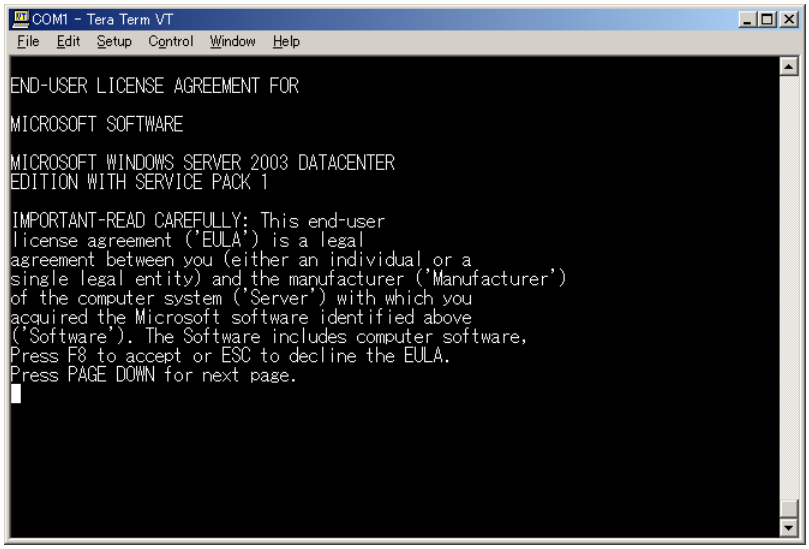

COM1 - Tera Term VT
File Edit Setup Control Window Help
END-USER LICENSE AGREEMENT FOR
MICROSOFT SOFTWARE
MICROSOFT WINDOWS SERVER 2003 DATACENTER
EDITION WITH SERVICE PACK 1
IMPORTANT-READ CAREFULLY: This end-user
license agreement ('EULA') is a legal
agreement between you (either an individual or a
single legal entity) and the manufacturer ('Manufacturer')
of the computer system ('Server') with which you
acquired the Microsoft software identified above
('Software'). The Software includes computer software,
Press F8 to accept or ESC to decline the EULA.
Press PAGE DOWN for next page.

Abbildung 3.23 Zustimmung zur Software-Lizenz

4 Geben Sie den Produktschlüssel ein und drücken Sie dann die [Enter]-Taste, wenn der folgende Bildschirm erscheint.
Wenn Sie danach zur Eingabe des Kennworts aufgefordert werden, geben Sie ein Kennwort ein und drücken Sie die [Enter]-Taste. (Dieses Fenster erscheint nur bei kundenspezifischer Installation).

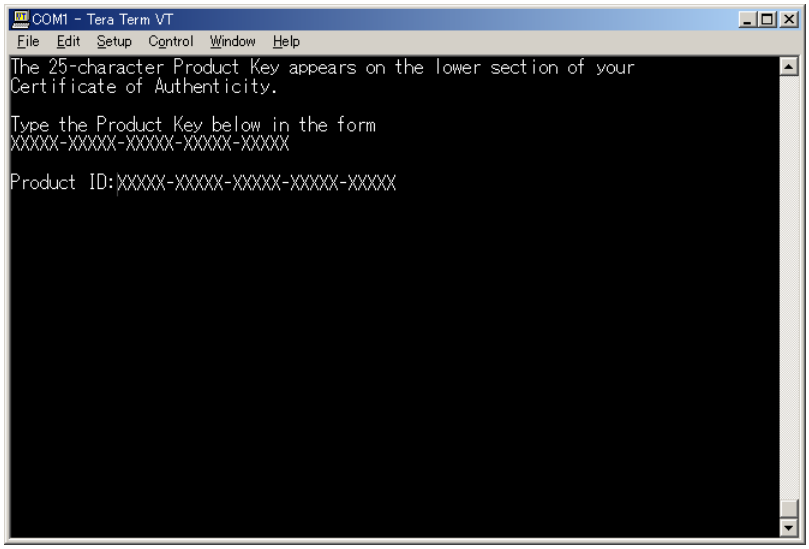

COM1 - Tera Term VT
File Edit Setup Control Window Help
The 25-character Product Key appears on the lower section of your
Certificate of Authenticity.
Type the Product Key below in the form
XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
Product ID:XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

Abbildung 3.24 Eingabe des Produktschlüssels

5 Wenn der folgende Bildschirm erscheint, wird das Betriebssystem neu gestartet. Drücken Sie keine Tasten, bis es wieder hochgefahren ist. Der Neustart dauert zirka 15 Minuten.

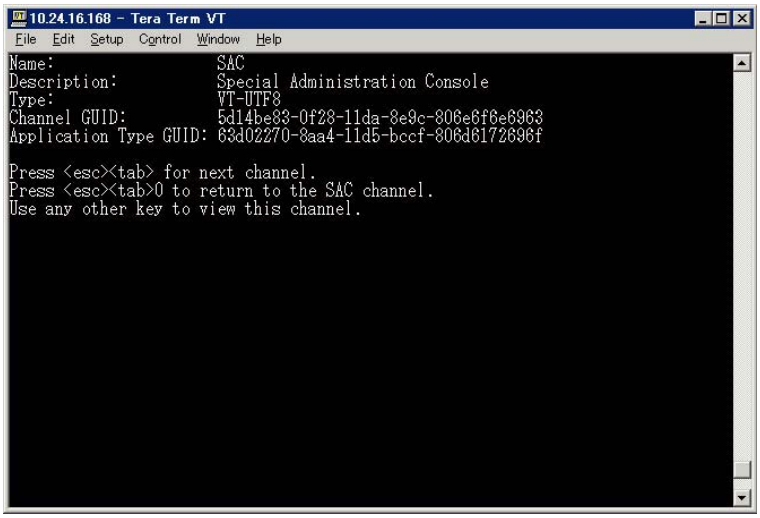

10.24.16.168 - Tera Term VT
File Edit Setup Control Window Help
Name: SAC
Description: Special Administration Console
Type: VT-UTF8
Channel GUID: 5d14be83-0f28-11da-8e9c-806e6f6e6963
Application Type GUID: 63d02270-8aa4-11d5-bccf-806d6172696f
Press <esc><tab> for next channel.
Press <esc><tab>0 to return to the SAC channel.
Use any other key to view this channel.

Abbildung 3.25 Neustart des Betriebssystems

3.3.5 Installation von Windows mit unabhängigem KVM-Switch (PRIMEQUEST 520A*/520/420)

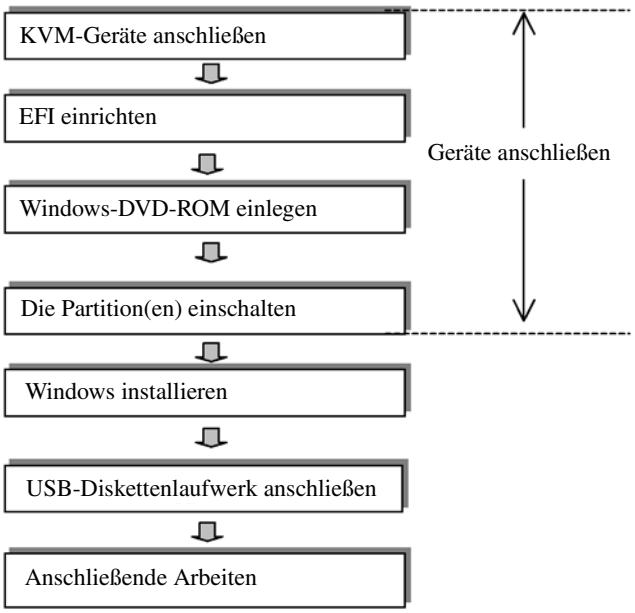
3.3.5.1 Hardwarevoraussetzungen und Verfahren

Die folgenden Geräte müssen angeschlossen sein, damit Windows mithilfe des unabhängigen KVM-Switches auf einem SAN-Laufwerk installiert werden kann:

- Unabhängiger KVM-Switch
- Tastatur
- Bildschirm
- Maus
- SAN-Speichereinheit (z.B. ETERNUS**)
- Fibre Channel-Karte
- LWL-Kabel
- Diskettenlaufwerk
  (muss separat vorbereitet werden. Wird während der Windows-Installation angeschlossen).

Anm.: Einzelheiten über den Anschluss der ETERNUS**-Einheiten an die PRIMEQUEST finden Sie im Handbuch des SAN-Speichers (z.B. ETERNUS**).

Die Installation umfasst folgende Schritte:



*: wird von Fujitsu Technology Solutions nicht unterstützt
**: Angebot und Support in EMEA nur für die globalen Kunden von Fujitsu

3.3.5.2 Geräte anschließen

Gehen Sie wie folgt vor, um den unabhängigen KVM-Switch an die IO Unit oder IOX der Partition anzuschließen, auf der Sie Windows installieren wollen:

(1) KVM-Einheit anschließen

1 Schließen Sie den unabhängigen KVM-Switch an den USB-Port und den VGA-Anschluss der IO Unit an.

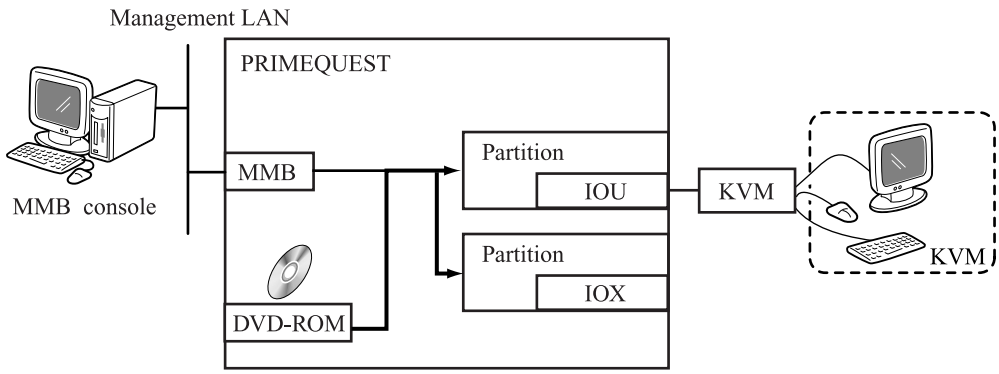


Abbildung 3.26 Installation mithilfe des unabhängigen KVM-Switches

2 Wählen Sie in der MMB Web-UI [Partition] → [DVD Switch].
Das Fenster [DVD Switch] wird angezeigt.
Anm.: Im 2.2.2.1, „An- und Abmelden bei der MMB Web-UI“ wird beschrieben, wie Sie sich beim MMB Web-UI anmelden.

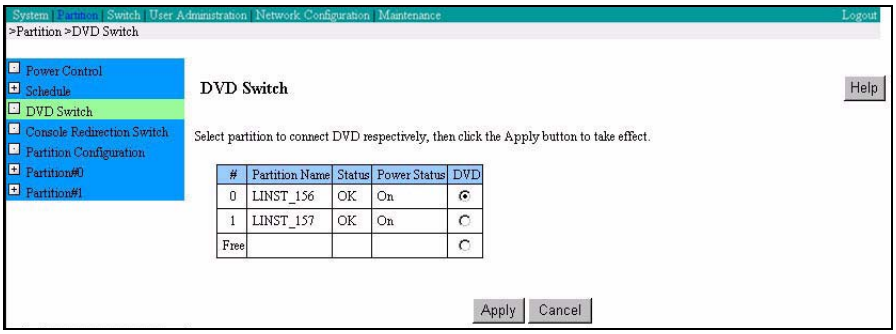


Abbildung 3.27 Das Fenster [DVD Switch]

3 Aktivieren Sie das Optionsfeld der Partition, auf der Sie das Betriebssystem installieren wollen und klicken Sie dann auf [Apply], um die Auswahl zu bestätigen.

3.3.5.3 Windows installieren

Dieser Abschnitt beschreibt, wie Sie Windows auf einem SAN-Laufwerk oder einem internen Laufwerk installieren.

1 Legen Sie die DVD-ROM mit Windows Server 2003 in das DVD-ROM-Laufwerk des OPL ein.

2 Wählen Sie im MMB Web-UI [Partition] → [Power Control].
Das Fenster [Power Control] wird angezeigt.

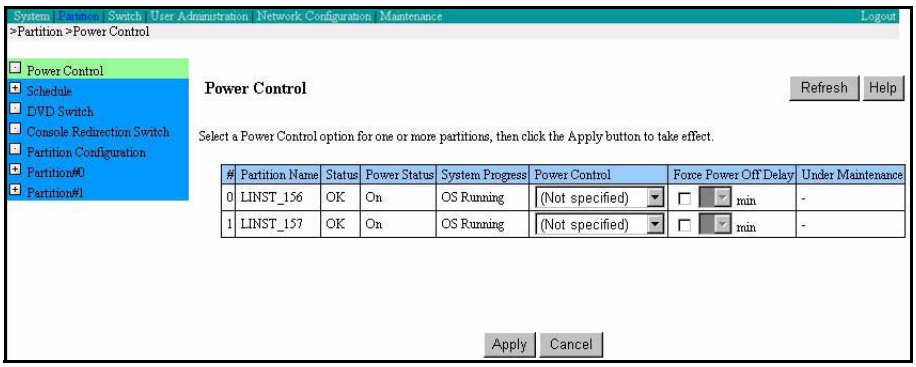

System | Partition | Switch | User Administration | Network Configuration | Maintenance
Logout
>Partition >Power Control
Power Control
Schedule
DVD Switch
Console Redirection Switch
Partition Configuration
Partition#0
Partition#1
Power Control
Refresh
Help
Select a Power Control option for one or more partitions, then click the Apply button to take effect.
| Partition Name | Status | Power Status | System Progress | Power Control | Force Power Off Delay | Under Maintenance
0 | LINST_156 | OK | On | OS Running | (Not specified) | min | -
1 | LINST_157 | OK | On | OS Running | (Not specified) | min | -
Apply
Cancel

Abbildung 3.28 Das Fenster [Power Control]

3 Wählen Sie in der Spalte [Power Control] der Partition, auf der Sie Windows installieren wollen, aus der Dropdown-Liste [Power On], um sie einzuschalten.
Anm.: Wenn die Partition bereits eingeschaltet ist, wählen Sie [Reset].

- Installation auf einer SAN-Speichereinheit, z.B. ETERNUS*
  Benutzen Sie den Fibre Channel-Kartentreiber (FC Driver), den Sie auf der CD „PRIMEQUEST Drivers CD for Microsoft® Windows Server® 2003“ (C122-E024) finden (in diesem Handbuch Treiber-CD genannt).
  Bereiten Sie die Treiber-Diskette auf einem separaten Windows-PC vor.

- Treiber-Diskette für Fibre Channel vorbereiten
  1 Formatieren Sie eine Diskette.
  2 Legen Sie die Treiber-CD in das CD-Laufwerk des separaten PCs.
  3 Öffnen Sie in einem Explorer-Fenster den folgenden Ordner auf der Treiber-CD:
  E:\Drivers\FC\Emulex (wenn E das CD-ROM-Laufwerk ist)
  4 Markieren Sie alle Dateien im Ordner und kopieren Sie sie auf die Diskette.

*: Angebot und Support in EMEA nur für die globalen Kunden von Fujitsu

- Installation auf einem über SCSI-Bus angeschlossenen Laufwerk
  Benutzen Sie den SCSI-Treiber, den Sie auf der „PRIMEQUEST Drivers CD for Microsoft® Windows Server® 2003“ (C122-E024) finden (in diesem Handbuch Treiber-CD genannt).
  Bereiten Sie die Treiber-Diskette auf einem separaten Windows-PC vor.

- Treiber-Diskette für SCSI vorbereiten
  1 Formatieren Sie eine Diskette.
  2 Legen Sie die Treiber-CD in das CD-Laufwerk des separaten PCs.
  3 Öffnen Sie in einem Explorer-Fenster den folgenden Ordner auf der Treiber-CD:
  E:\Drivers\SCSI\LSILogic (wenn E das CD-ROM-Laufwerk ist)
  4 Markieren Sie alle Dateien im Ordner und kopieren Sie sie auf die Diskette.

- Installation auf einem integrierten SAS-Laufwerk
  Benutzen Sie den SAS-Treiber, den Sie auf der „PRIMEQUEST Drivers CD for Microsoft® Windows Server® 2003“ (C122-E024) finden (in diesem Handbuch Treiber-CD genannt).
  Bereiten Sie die Treiber-Diskette auf einem separaten Windows-PC vor.

- Treiber-Diskette für SAS vorbereiten
  1 Formatieren Sie eine Diskette.
  2 Legen Sie die Treiber-CD in das CD-Laufwerk des separaten PCs.
  3 Öffnen Sie in einem Explorer-Fenster den folgenden Ordner auf der Treiber-CD:
  E:\drivers\SAS\LSIlogic (wenn E das CD-ROM-Laufwerk ist)
  4 Markieren Sie alle Dateien im Ordner und kopieren Sie sie auf die Diskette.

4 Klicken Sie auf [Apply], um die Einstellung zu bestätigen.
  Die Meldung [EFI Boot Manager] wird auf der Konsole angezeigt, die mit dem KVM-Gerät verbunden ist.

```
EFI Boot Manager  ver 1.xx [xx.xx]

Please Select a boot option
DVD /Acpi(xxxxxxxx)
Network Boot/Pci(1|0|0)/Mac(0007E9D80F36)
EFI Shell [Built in]
Boot option maintenance menu
```

Hinweis: Stellen Sie sicher, dass das USB-Diskettenlaufwerk nicht installiert ist. Wenn sich eine Diskette im USB-Laufwerk befindet, erscheint möglicherweise die unten wiedergegebene Meldung.

```
INF file txtsetup is corrupt or missing,status 18.
Setup cannot continue. Press any key to exit.
```

Drücken Sie in dem Fall die [Enter]-Taste, damit Windows neu starten kann. Ziehen Sie den Anschluss des USB-Diskettenlaufwerks heraus und stecken Sie ihn dann wieder ein. Fahren Sie daraufhin mit Schritt 4 in diesem Installationsprozess fort.
Wenn Windows nicht neu startet, nachdem Sie die [Enter]-Taste gedrückt haben, ziehen Sie den Anschluss des USB-Diskettenlaufwerks heraus, stecken Sie ihn dann wieder ein und fahren Sie mit Schritt 2 fort. Schließen Sie das USB-Diskettenlaufwerk an den PC an, wenn Sie die Treiber manuell installieren.

5 Wählen Sie „DVD /Acpi (xxxxxxxx)“ und drücken Sie die [Enter]-Taste.
Wenn der Festplatte ein aktiver Bereich zugewiesen wurde, erscheint die folgende Meldung. Drücken Sie, während diese Meldung angezeigt wird, eine beliebige Taste, um das System vom DVD-ROM-Laufwerk aus zu laden.

```
Press any key to boot from CD ... .
```

6 Der Installationsbildschirm von Windows Server 2003 wird angezeigt.
Unten auf dem Installationsbildschirm erscheint sofort nach dessen Anzeige die folgende Meldung. Diese Meldung wird für kurze Zeit unmittelbar nach dem Setup Screen (blue screen) angezeigt. Drücken Sie sofort die [F6]-Taste, nachdem der Setup Screen (blue screen) angezeigt wurde.

```
Press F6 if you need to install third party
SCSI or RAID driver ... .
```

7 Installieren Sie den Treiber manuell.

1 Drücken Sie die [S]-Taste, wenn die folgende Meldung erscheint:

```
To specify additional SCSI adapters, CD-ROM drivers,
or special disk controllers for use with Windows,
including those for which you have a device support
disk from mass storage device manufacturer, press S
```

2 Wenn die folgende Meldung erscheint, schließen Sie das USB-Diskettenlaufwerk an.

```
Please insert disk labeled Manufacture-supplied hard-
ware support disk into Drive A:
```

Um das Laufwerk an die IO Unit anzuschließen, verbinden Sie es mit dem USB-Port auf der linken Seite von der Rückseite der Systemeinheit aus gesehen.

Um es an IOX anzuschließen, verbinden Sie es mit dem USB-Port darunter.

3 Legen Sie die in Schritt 3 vorbereitete Treiberdiskette in das Diskettenlaufwerk ein.

4 Drücken Sie die [Enter]-Taste. Die folgende Meldung erscheint:

```
You have chosen to configure a SCSI adapter for use
with Windows, using a device support disk provided by
an adapter manufacturer. Select the SCSI adapter you
want from the following list, or press ESC to return
the previous screen
```

5 Wählen Sie die folgende Option aus und drücken Sie die [Enter]-Taste:

- Fibre Channel

```
Emulex LPX000 PCI Fibre Channel HBA
```

- SCSI

```
LSI Logic PCI Fusion-MPT Driver (Server 2003 IA64)
```

- SAS

```
LSI Logic Fusion-MPT SAS Driver (Server 2003 IA64)
```

Hinweis: Entfernen Sie das Disketten-Laufwerk nicht, bevor die Installation beendet ist.

8 Fahren Sie mit der Installation fort, indem Sie den Anweisungen des Installationsprogramms folgen.
Weitere Einzelheiten finden Sie im Handbuch des Betriebssystems.
Wird in einer Meldung im Verlauf der Installation eine Diskette verlangt, dann legen Sie die Treiber-Diskette ein und drücken Sie die [Enter]-Taste.
Anm.: Während der Installation wird die Produktkennung angefordert. Je nach Betriebssystem und Kaufverfahrenfinden Sie diese an einer anderen Stelle.

Tabelle 3.11 Produktkennungen

Betriebssystem	Kaufverfahren	Produktkennung
Windows Server 2003, Enterprise Edition für Itanium-basierte Systeme	Datenträger-Lizenz	CD-Paket mit den Medien für das Betriebssystem
	zusammen mit der Hardware	CoA-Etikett auf der Systemeinheit oder einer separaten Einheit (*1)(*2)(*3)
Windows Server 2003, Datacenter Edition für Itanium-basierte Systeme	zusammen mit der Hardware	CoA-Etikett auf der Systemeinheit oder einer separaten Einheit (*1)(*2)(*4)

*1:Lesen Sie die „Important Notice“ der Systemeinheit, um zu erfahren, wo sich das CoA-Etikett mit der Produktkennung befindet.
*2:Wenn das CoA-Etikett eine separate Einheit ist, lesen Sie unbedingt die „Important Notice“, die zu deren Lieferumfang gehört, und bringen Sie das Etikett dann auf der Systemeinheit an.
*3:Verwenden Sie ein CoA-Etikett, das mit „Enterprise“ gekennzeichnet ist. Gibt es mehrere CoA-Etikette mit dieser Kennzeichnung, müssen Sie darauf achten, dass Sie während der Installation ausschließlich eine Produktkennung verwenden.
*4:Verwenden Sie ein CoA-Etikett für Datacenter, das mit „4 CPU“ gekennzeichnet ist.

9 Starten Sie das System neu. Im Bildschirm des EFI Boot Manager wurde „Windows Server 2003, Datacenter“ oder „Windows Server 2003, Enterprise Edition“ hinzugefügt. Wählen Sie diese Option des Boot-Menüs aus, um Windows zu starten.

3.3.5.4 Bedienerlose Installation

Mit dem Emergency Management Service (EMS) von Windows Server 2003 ist eine bedienerlose Installation über KVM möglich. Sie brauchen hierzu ein COM-Kabel und einen Notebook-PC mit COM-Port.

Stellen sie sicher, dass im Fenster [Console Redirection Switch] in der Auswahl [Partition] im MMB Web-UI als Partition, auf der Sie Windows installieren wollen, „COM“ angegeben ist.

Hinweise zur bedienerlosen Installation

- Das COM-Kabel muss an den COM-Port der IO Unit angeschlossen werden.
- Tastatureingaben für die Terminalsoftware weichen von jenen für die Bildschirmeingabe ab.
  Wenn das Installationsprogramm Sie beispielsweise auffordert, eine Funktionstaste [Fx] zu drücken, drücken Sie die [ESC]-Taste und dann die Taste mit der Ziffer „x“.
  Wenn das Installationsprogramm Sie auffordert, die [Bild nach unten]-Taste zu drücken, drücken Sie die [ESC]-Taste und dann die [/]-Taste.
  Wenn das Installationsprogramm Sie auffordert, die [Bild nach oben]-Taste zu drücken, drücken Sie die [ESC]-Taste und dann die [?]-Taste.

  Hinweis: Drücken Sie die Zifferntaste, [/]-Taste bzw. [?]-Taste sofort nach der [ESC]-Taste. Wenn der zeitliche Abstand zwischen der Betätigung der [ESC]-Taste und der zweiten Taste zu lang ist, erkennt das System eventuell nur die [ESC]-Taste und interpretiert den Tastendruck als Befehl zum Neustart.

- Wählen Sie den Tastaturtyp wie folgt aus:

1 Drücken Sie die [s]-Taste, wenn der Auswahlbildschirm für den Tastaturtyp angezeigt wird.

```
Press one of the following keys to select a keyboard
type:

en-size/em-size key: 106 Japanese keyboard
Space key: 101 English keyboard
"S" key: Other keyboard

-  To quit setup, press the [F3] key.
```

2 Mit 101 wählen Sie die englische Tastatur aus.

```
Select a keyboard type from the following list:

-  To continue setup, press the [Enter] key.
-  To quit setup, press the [F3] key.

  +-------------------------------------------------+
  | 106 Japanese Keyboard (Including USB)           |
  | 101 English Keyboard (Including USB)            |
  | NEC 98 Layout USB Keyboard                      |
  | USB Keyboard                                    |
  +------------------------------(Scroll down  )--+
```

- Verwenden Sie eine Terminalanschluss-Software, die UTF-8 unterstützt.
  Eine Terminalanschluss-Software, die UTF-8 nicht unterstützt, zeigt Zeichen möglicherweise fehlerhaft an.

Installation

Verwenden Sie eine Terminalanschluss-Software, um eine Verbindung herzustellen. Als Standardsoftware wird mit Windows XP HyperTerminal bereitgestellt. Das Beispiel in diesem Abschnitt verwendet Tera Term.

Stellen Sie eine Datenübertragungssoftware wie folgt ein:

Tabelle 3.12 Terminalsoftware-Einstellungen

Parameter	Wert
Bits/second	19200
Data bits	8
Parity	None
Stop bit	1
Flow control	None
Emulation	VT100

Bereiten Sie Treiber-Disketten gemäß Schritt 3 in 3.3.4.3, „Windows installieren“ vor. Wenn die Anzeigen auf dem blauen Bildschirm komplett ist, nehmen Sie die im Folgenden beschriebenen Einstellungen vor.

1 Starten Sie Tera Term. Drücken Sie die [ESC]- und die [TAB]-Taste, wenn der folgende Bildschirm erscheint.

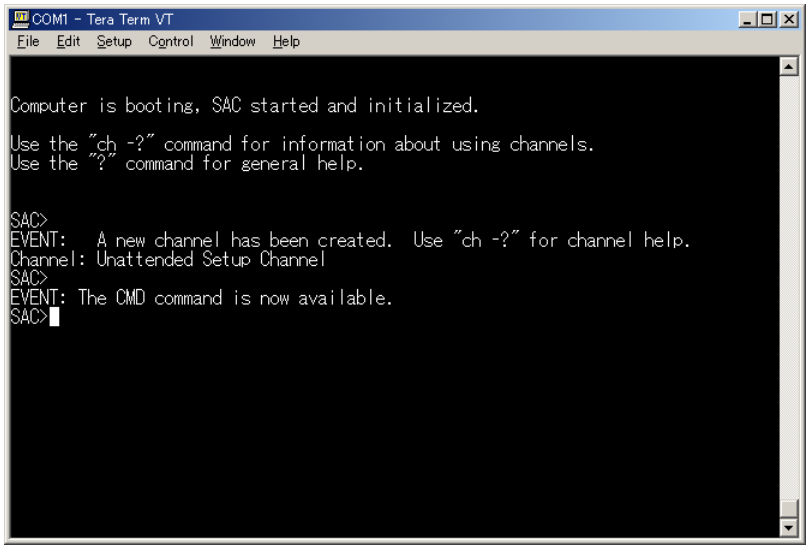

COM1 - Tera Term VT
File Edit Setup Control Window Help
Computer is booting, SAC started and initialized.
Use the "ch -?" command for information about using channels.
Use the "?" command for general help.
SAC>
EVENT: A new channel has been created. Use "ch -?" for channel help.
Channel: Unattended Setup Channel
SAC>
EVENT: The CMD command is now available.
SAC>

Abbildung 3.29 Tera Term-Startfenster

2 Drücken Sie die [Enter]-Taste, wenn der folgende Bildschirm erscheint.

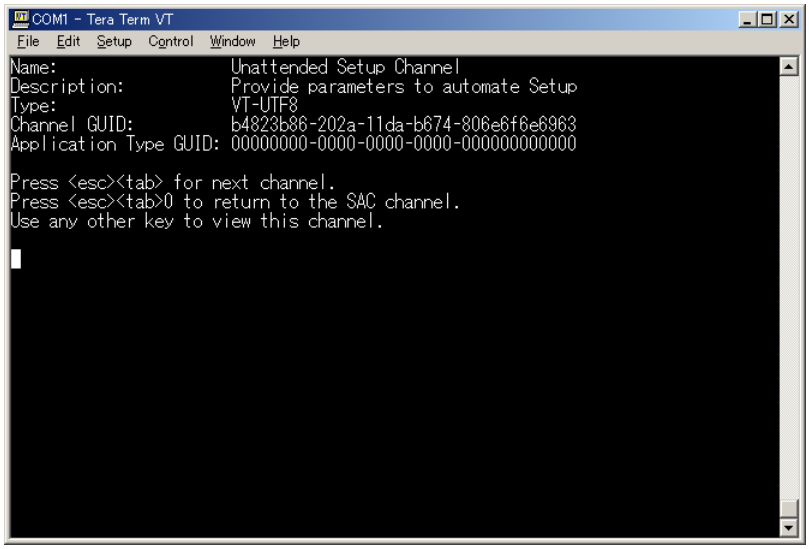

COM1 - Tera Term VT
File Edit Setup Control Window Help
Name: Unattended Setup Channel
Description: Provide parameters to automate Setup
Type: VT-UTF8
Channel GUID: b4823b86-202a-11da-b674-806e6f6e6963
Application Type GUID: 00000000-0000-0000-0000-000000000000
Press <esc><tab> for next channel.
Press <esc><tab>0 to return to the SAC channel.
Use any other key to view this channel.

Abbildung 3.30 Setup-Fenster

3 Drücken Sie die [ESC]-Taste und die [8]-Taste, wenn der folgende Bildschirm erscheint.

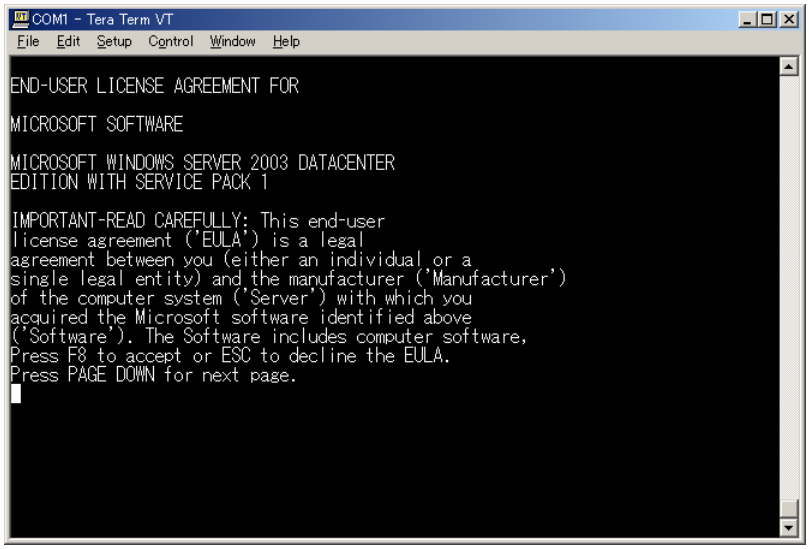

COM1 - Tera Term VT
File Edit Setup Control Window Help
END-USER LICENSE AGREEMENT FOR
MICROSOFT SOFTWARE
MICROSOFT WINDOWS SERVER 2003 DATACENTER
EDITION WITH SERVICE PACK 1
IMPORTANT-READ CAREFULLY: This end-user
license agreement ('EULA') is a legal
agreement between you (either an individual or a
single legal entity) and the manufacturer ('Manufacturer')
of the computer system ('Server') with which you
acquired the Microsoft software identified above
('Software'). The Software includes computer software,
Press F8 to accept or ESC to decline the EULA.
Press PAGE DOWN for next page.

Abbildung 3.31 Zustimmung zur Software-Lizenz

4 Geben Sie die Produktkennung ein und drücken Sie dann die [Enter]-Taste, wenn der folgende Bildschirm erscheint.
Wenn Sie danach zur Eingabe des Kennworts aufgefordert werden, geben Sie ein Kennwort ein und drücken Sie die [Enter]-Taste. (Dieses Fenster erscheint nur bei kundenspezifischer Installation).

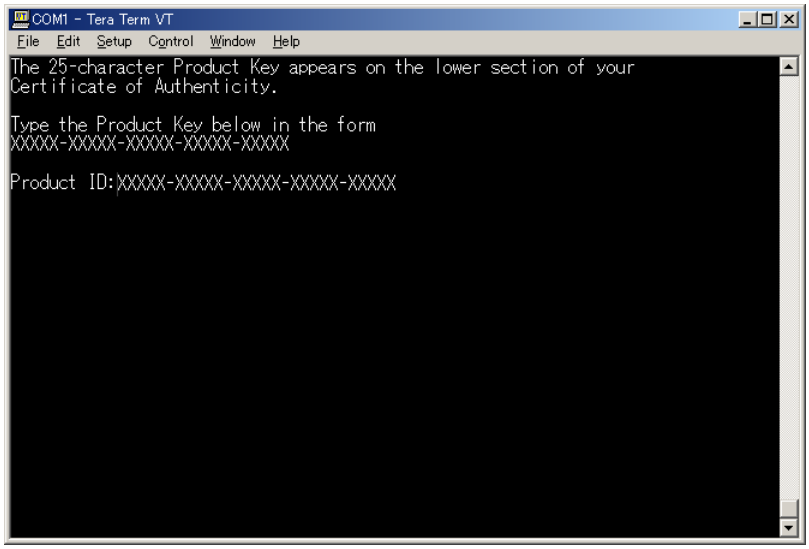

COM1 - Tera Term VT
File Edit Setup Control Window Help
The 25-character Product Key appears on the lower section of your
Certificate of Authenticity.
Type the Product Key below in the form
XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
Product ID:XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

Abbildung 3.32 Eingabe der Produktkennung

5 Wenn der folgende Bildschirm erscheint, wird das Betriebssystem neu gestartet. Drücken Sie keine Tasten, bis es wieder hochgefahren ist. Der Neustart dauert zirka 15 Minuten.

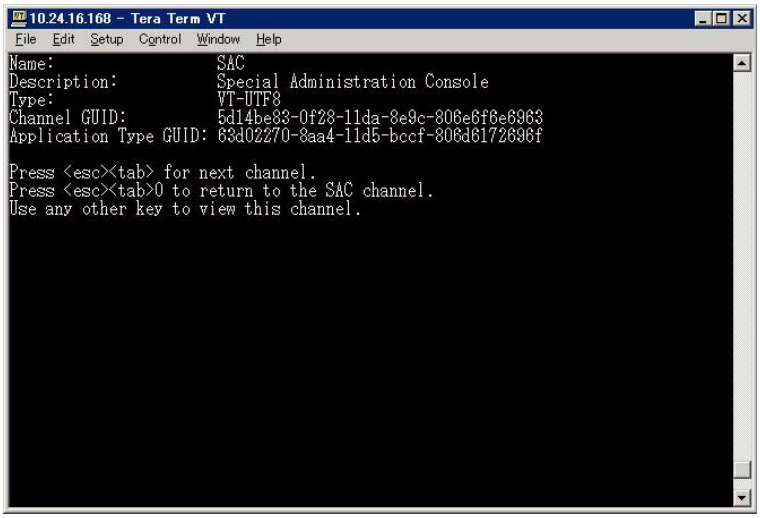

10.24.16.168 - Tera Term VT
File Edit Setup Control Window Help
Name: SAC
Description: Special Administration Console
Type: VT-UTF8
Channel GUID: 5d14be83-0f28-11da-8e9c-806e6f6e6963
Application Type GUID: 63d02270-8aa4-11d5-bccf-806d6172696f
Press <esc><tab> for next channel.
Press <esc><tab>0 to return to the SAC channel.
Use any other key to view this channel.

Abbildung 3.33 Neustart des Betriebssystems

3.3.6 High Reliability Tools

Die Treiber-CD enthält Treiber und Anwendungen, die einen stabilen Betrieb gewährleisten. Sie werden als High Reliability Tools bezeichnet.

Die High Reliability Tools können abhängig von der Windows-Installation unterschiedlich installiert werden:

- Windows-Installation mit SystemcastWizard Lite
  Die High Reliability Tools werden automatisch installiert.
- Windows-Installation mit Installation Support Tool for Windows
  Nach der Windows-Installation muss die Treiber-CD mit den High Reliability Tools manuell in das DVD-ROM-Laufwerk eingelegt werden. Die High Reliability Tools werden dann automatisch installiert.
- Windows-Installation mit KVM
  Die High Reliability Tools müssen nach der Windows-Installation manuell installiert werden.

3.3.6.1 Installation mit PRIMEQUEST Software Installer

Der PRIMEQUEST Software Installer überprüft automatisch, ob die erforderlichen Tools vorhanden sind und installiert fehlende Tools automatisch. Der Installer installiert die aktuellsten Treiber. In diesem Abschnitt wird eine Installation mit dem PRIMEQUEST Software Installer beschrieben.

1 Melden Sie sich bei der relevanten Partition mit Windows-Betriebssystem als Benutzer mit Systemverwalterrechten an (z.B. administrator).

2 Legen Sie die Treiber-CD in das DVD-ROM-Laufwerk:
In Abhängigkeit vom Servermodell ist das DVD-ROM-Laufwerk:
- PRIMEQUEST 580/540/480/440: DVD-ROM-Laufwerk des KVM
- PRIMEQUEST 520/420: OPL DVD-ROM-Laufwerk

3 Wählen Sie [Start] → [Run]. Das Dialogfeld [Run] wird angezeigt.

4 Geben Sie im Feld [Name] folgendes ein und klicken Sie dann auf [Run]:
DVD-ROM-Laufwerk:\pqsetup.exe

Der PRIMEQUEST Software Installer startet, und folgendes Fenster wird angezeigt.

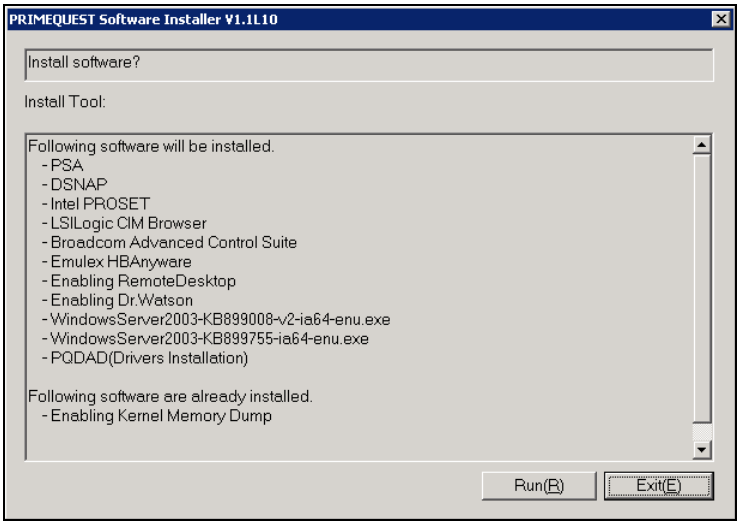


Abbildung 3.34 High-Reliability Tools Installer: Startfenster

5 Überprüfen Sie noch einmal die unter [Install Tool:] aufgeführten Tools und Treiber und klicken Sie auf die Schaltfläche [Run].
Die High-Reliability-Tools und Treiber werden jetzt installiert.
Gegebenenfalls wird eine weitere Bestätigung gefordert, bevor die Installation fortgesetzt wird.

6 Wenn die Installation abgeschlossen ist, klicken Sie auf die Schaltfläche [Exit].

7 Starten Sie die Partition neu, um die Installation abzuschließen.
Die Installation mit PRIMEQUEST Software Installer ist nun abgeschlossen.

Anm.: Logdateien werden in den folgenden Verzeichnissen erstellt:

- Ergebnisse der Software-Installation
  %systemroot%\system32\LogFiles\PQSetup.log
- Ergebnisse der Treiber-Installation
  %systemroot%\system32\LogFiles\pqdad-yyyymmdd.log
  yyyymmdd: Jahr-Monat-Tag, an dem der Treiber installiert wurde.

Tabelle 3.13 Von PRIMEQUEST Software Installer installierte Tools und Treiber

Software-Produkt/ Installationspaket	Beschreibung
Tools	
PSA	SNMP muss vorher installiert sein. Näheres finden Sie in 3.3.6.2, „Anmerkungen zum PRIMEQUEST Software Installer“.
SIRMS	Installation nur unter einer japanischen Version von Windows. Näheres finden Sie in 3.3.6.2, „Anmerkungen zum PRIMEQUEST Software Installer“.
SIRMS MNS	Installation nur unter einer japanischen Version von Windows. Näheres finden Sie in 3.3.6.2, „Anmerkungen zum PRIMEQUEST Software Installer“.
DSNAP	Support-Werkzeug
HRM/server	Tool zur Wartungsunterstützung
Software Support Guide	Tool zur Sammlung erforderlicher Support-Informationen.
Treiber	
Intel LAN Driver	Unterstützter Intel LAN-Treiber
BroadCom LAN Driver	On-Board LAN-Treiber
Neterion LAN Driver	Unterstützter Neterion LAN-Treiber
Emulex FC Driver	Fibre Channel-Treiber
LSI Logic SCSI Driver	SCSI-Treiber
LSI Logic SAS Driver	On-Board SAS-Treiber für PRIMEQUEST 520/420
HP DAT72 Driver	DAT72-Treiber
TANDBERG LTO2 Driver	LTO2-Treiber
Quantum LTO3 Driver	LTO3-Treiber
Treiberverwaltungswerkzeug	
Intel PROSet	Intel LAN Load Balance-Funktion, usw.
BroadCom Advanced Controller Suite(BACS)	On-Board LAN-Treiber mit Load Balance-Funktion

Software-Produkt/ Installationspaket	Beschreibung
Xframe Control Panel	Versorgung des Neterion LAN-Treibers mit Load Balance-Funktionen
Emulex HBAnyware	Überwachung des LUN-Status über Fibre Channel-Verbindung.
Windows Patch	
KB899008	Patch für Windows Server 2003 Enterprise Edition für Itanium-basierte Systeme.
KB899755	IA32-EL Patch
KB244139	Erweiterung um eine Tastaturfunktion für einen Memory Dump
KB899416	Patch zur Korrektur von gelegentlich auftretendem beschädigten Event Log
KB919385	Patch zur Unterstützung des Dual-Core Intel Itanium2 Prozessors
KB932755	Storport Driver Patch
Installation	
Enabling RemoteDesktop	Installiert automatisch einen Remote Desktop für eine entfernte Verwaltung.
Enabling Kernel Memory Dump	Nimmt automatisch Dump-Einstellungen für den Fehlerfall vor.
PXH setting change	Nimmt PXH-Einstellungen vor.
PEX setting change	Nimmt PEX-Einstellungen vor.

3.3.6.2 Anmerkungen zum PRIMEQUEST Software Installer

- Für die Installation des PSA benötigen Sie die Windows Server 2003 DVD-ROM. SNMP muss für die Installation des PSA bereits vorhanden sein. Wenn SNMP noch nicht installiert ist, gibt der PRIMEQUEST Software Installer eine Meldung aus, in der der Benutzer aufgefordert wird, die Windows Server 2003 DVD-ROM einzulegen und SNMP zu installieren. Legen Sie die Windows Server 2003 DVD-ROM für die Installation bereit.
- Intel PROSet und Xframe Control Panel werden nicht automatisch installiert.
  Intel PROSet und Xframe Control Panel werden nicht automatisch installiert. Es befindet sich im Ordner „Not_installed“ auf dem Desktop. Installieren Sie dieses Werkzeug manuell.
- Treiber/Tools werden nur installiert, wenn deren Geräte erkannt werden.
  Treiber und die zugehörigen Tools werden nur dann installiert, wenn die relevanten Geräte (LAN-Karten, Fibre Channel-Karten, usw.) in der IO Unit der Partition installiert sind.
- SIRMS, SIRMS MNS und HRM/server werden nur unter der japanischen Version von Windows installiert.

- Während der Installation werden möglicherweise einige Meldungen angezeigt. Wenn während der Installation in einem Dialogfenster mitgeteilt wird, dass ein Treiber keine Windows-Abnahme besitzt, klicken Sie auf [Yes], um den Installationsvorgang fortzusetzen.
- Einige installierte Tools sind ggf. ihrerseits wieder Installationsziele. Obwohl der PRIMEQUEST Software Installer diese Tools bereits installiert hat, kann es sein, dass er sie erneut installiert. Dies stellt aber kein Problem dar.

3.3.7 Erforderliche Arbeiten nach der Installation

3.3.7.1 Einstellung des Bildschirmtreibers (Serie PRIMEQUEST 500A*/ 500)

Wird der ATI RAGE XL Display-Treiber, der im gleichen Paket wie Microsoft® Windows Server® 2003 Enterprise Edition ausgeliefert wird, in einem Gerät der Serie PRIMEQUEST 500A*/500 benutzt, tritt evtl. das gleiche Problem auf, das in der Technischen Information KB924897 von Microsoft beschrieben ist. Um den Standard-VGA-Treiber nutzen zu können, führen Sie nachfolgende Prozedur durch. Benötigen Sie hohe Auflösung, etwa zur Installation einer Anwendung, verwenden Sie die Funktion „Remote Desktop“.

1 Wählen Sie [Control Panel] → [System].

2 Wählen Sie das Registerblatt [Hardware], und starten Sie den Device Manager.

3 Wählen Sie „RAGE XL PCI Family“ aus dem Display Adapter, klicken Sie mit der rechten Maustaste darauf, und wählen Sie anschließend [Disable] aus dem Menu.

4 Starten Sie das System gemäß den angezeigten Anweisungen neu.

*: wird von Fujitsu Technology Solutions nicht unterstützt

3.3.7.2 Installation des Multipath-Treibers

Nachdem Sie das Betriebssystem in einer 1-Pfad-Umgebung installiert haben, führen Sie die Fibre Channel-Verkabelung in einer Multipath-Umgebung durch. Installieren Sie den Multipath-Treiber, und führen Sie anschließend die Verkabelung in der Multipath-Umgebung durch.

Hinweise:

- Bauen Sie keine Multipath-Verbindung zwischen der PRIMEQUEST-Maschine und SAN-Speichereinheiten auf, ohne vorher den Multipath-Treiber installiert zu haben. Ansonsten könnten Daten beschädigt werden. Weitere Einzelheiten über Multipath-Treiber und Multipath-Verbindung finden Sie im Handbuch *ETERNUS* Multipath Driver V2.0 User's Guide for Windows(R)*.
- Installieren Sie den ETERNUS-Gerätetreiber, wenn Sie das System in einer Siglepath-Umgebung einsetzen wollen. Einzelheiten finden Sie unter folgender URL zum ETERNUS*-Gerätetreiber und GR-Gerätetreiber: http://storage-system.fujitsu.com/jp/download/grdvdr/

3.3.7.3 Plattenlaufwerk wieder einsetzen

Wurde das SCSI/SAS Plattenlaufwerk für Daten vor der Installation des Betriebssystems entfernt, setzen Sie es an seinem ursprünglichen Platz wieder ein. Nach der Konfigurierung der für das System vorgesehenen Umgebung starten Sie das Betriebssystem.

Damit ist die Installation von Windows beendet.

Installieren Sie den ETERNUS*-Gerätetreiber, wenn Sie das System in einer Siglepath-Umgebung einsetzen wollen.

*: Angebot und Support in EMEA nur für die globalen Kunden von Fujitsu

KAPITEL 4 Nach Installation des Betriebssystems erforderliche Arbeiten

4.1 Art der erforderlichen Arbeiten

Dieses Kapitel beschreibt die Aufgaben, die nach der Installation des Betriebssystems durchgeführt werden müssen.
Die folgende Tabelle führt diese Aufgaben in einem Überblick auf und gibt an, in welchem Abschnitt des Kapitels sie jeweils beschrieben sind.

Tabelle 4.1 Erforderliche Aufgaben

Aufgaben	Beschreibung	Betriebssystem	Modell	Abschnitt
PSA-Installation	PSA installieren.	Linux (Red Hat)	PRIMEQUEST 580A/540A*/580/540/480/440	4.2
			PRIMEQUEST 520A*/520/420	4.2.6
		Linux (SUSE)	PRIMEQUEST 500A/500/400- Modellreihe	4.4
		Windows	PRIMEQUEST 580A/540A*/580/540/480/440	4.5
			PRIMEQUEST 520A*/520/420	4.6
Einrichten der PSA-Überwachung	S.M.A.R.T. bzw. Watchdog einrichten.	Linux oder Windows	PRIMEQUEST 500A/500/400-Modellreihe	4.8
Einrichten der Dump-Umgebung	Dump-Umgebung einrichten.	Linux (nur Red Hat)	PRIMEQUEST 500A/500/400-Modellreihe	4.9
		Windows	PRIMEQUEST 500A/500/400-Modellreihe	4.10
Einrichten der NTP Clients	NTP-Clients einrichten.	Linux oder Windows	PRIMEQUEST 500A/500/400-Modellreihe	4.11

Aufgaben	Beschreibung	Betriebs-system	Modell	Abschnitt
Sicherung des Betriebssystems	Sicherung von Linux einstellen	Linux (nur Red Hat)	PRIMEQUEST 500/400-Modellreihe	4.12.1
	Sicherung von Windows einstellen	Windows	PRIMEQUEST 500/400-Modellreihe	4.12.2
Sicherung der Einstellungen	PSA-Einstellungen und EFI-Konfiguration sichern.	Linux oder Windows	PRIMEQUEST 500A/500/400-Modellreihe	4.13

*: wird von Fujitsu Technology Solutions nicht unterstützt

Anm.: Wenn Sie unter Linux (Red Hat) oder Windows den PSA (PRIMEQUEST Server Agent) installieren, werden dabei die für REMCS* erforderlichen bnetriebssystemnahen Komponenten installiert. Die REMCS*-Konfiguration wird vom Techniker durchgeführt.
Neben der Installation des PSA muss auch die PSA-Überwachung eingestellt werden.

*: wird von Fujitsu Technology Solutions nicht unterstützt

4.2 PSA installieren (Linux: Red Hat) (PRIMEQUEST 580A/540A*/580/540/480/440)

In diesem Abschnitt werden die Punkte beschrieben, die vor Installation des PSA überprüft werden müssen.

Obligatorische Aufgaben:

- Einstellungen des Management-LANs überprüfen (→ 4.2.1)
- Einstellungen für SELinux überprüfen (→ 4.2.2)
- Firewall überprüfen (Ports freigeben) (→ 4.2.3)
- FJSVfefpcl installieren (→ 4.2.4)

Optionale Aufgaben:

- Ziel für Partition-Traps festlegen (→ 4.3.5)
- Ziel für Traps und E-Mails über MMB festlegen (→ 4.3.6)
- Sonstige Einstellungen (→ 4.2.7)

Anm.:

- Benutzen Sie das PRIMEQUEST Installation Support Tool, den Installer für Software-Bundle-Packages oder SystemcastWizard Lite, um den PSA zu installieren. Wie Sie den PSA manuell installieren können, ist in Kapitel 4, „Manual PSA Installation“ im Handbuch *PRIMEQUEST 500A/500/400 Series Reference Manual: Tools/Operation Information* (U41757-J-Z816-x-76/C122-E074EN) beschrieben.
  Das PRIMEQUEST Installation Support Tool ist im *PRIMEQUEST Installation Support Tool User's Guide (Red Hat)* (C122-E005EN) beschrieben.
  Einzelheiten über den Installer für Software-Bundle-Packages finden Sie im *PRIMEQUEST Bundled-Software Package Installer User's Guide* (C122-E006EN).
  Näheres über SystemcastWizard Lite finden Sie im *PRIMEQUEST SystemcastWizard Lite User's Guide* (C122-E010EN).
- Während der Installation des PSA werden die folgenden für den Betrieb erforderlichen Modifikationen automatisch durchgeführt:
  - Hinzufügen ~~**von**~~ **der** Einstellungen in der **Datei** syslog.conf
  - Hinzufügen ~~**von**~~ **der** Einstellungen in der **Datei** snmpd.conf

*: wird von Fujitsu Technology Solutions nicht unterstützt

- ~~**Einrichten**~~ **Hinzufügen der Einstellungen in** der Datei snmptrapd.conf
- Deaktivierung der automatischen Starteinstellungen von salinfo oder salinfo_decode (*1)
- Deaktivierung der automatischen Starteinstellungen von smartd (*1)
- Einfügen der Beschreibung in die Datei services (*2)
- ~~**Korrekturen in scsi.agent (*3)**~~
- **Korrektur der Gerätetypen in der Datei scsi.agent (PSA1.16.2-xRHEL4 oder später) (*3)**
- **Hinzufügen der Einstellungen in der Datei crontab (PSA1.3.x-xRHEL4 bis PSA1.6.x-xRHEL4)**
- **Änderung der Boot-Option snmptrapd**

*1 Diese automatischen Starteinstellungen sind wegen Konflikten mit einigen PSA-Funktionen deaktiviert.

*2 Hinzugefügter Port:
Es wird nicht überprüft, ob Portnummern doppelt vorhanden sind, wenn ~~**weitere Daten**~~ **die Einstellungen** in die Dienstedatei fj-webgate (24450) eingefügt werden. Führen Sie eventuell notwendige Änderungen durch.

***3 Korrekturen werden nur unter RHEL-AS4 (IPF) vorgenommen.**

[Korrekturen (halbfett ausgezeichnet) gemäß Handbuch-Errata 2008/12/18 und 2009/02/24]

Anmerkung: Falls die IP-Adresse des MMB oder die des Management-LANs auf seiten der Partition geändert wurde, dürfen Sie nicht vergessen, PSA neu zu starten. Andernfalls kommt es zu einem Anzeigefehler im PSA-Fenster des MMB-Web-UI, und die von PSA registrierten Fehler werden nicht gemeldet.

4.2.1 Einstellungen des Management-LANs überprüfen

In diesem Abschnitt wird beschrieben, wie Sie die Einstellungen des Management-LANs überprüfen können.
Damit der PSA über das Management-LAN mit dem MMB kommunizieren kann, muss die mit dem Management-LAN verbundene NIC (Network Interface Card) der Partition aktiv sein.

(1) Einstellungen für die NIC des Management-LANs überprüfen

Führen Sie das folgende Kommando aus, um den Namen der Schnittstelle zu überprüfen, der dem NIC des Management-LANs zugewiesen ist.

1 Geben Sie das Kommando ifconfig ein, um die vom System erkannten Netzwerkschnittstellen aufzulisten und den betreffenden Schnittstellennamen zu bestätigen.
Kommandosyntax:

```
/sbin/ifconfig –a
```

Beispiel: Die Schnittstellen heißen eth0, eth1 und lo.

```
# /sbin/ifconfig –a
eth0      Link encap:Ethernet  HWaddr 00:D0:B7:53:89:C3
          inet addr:10.24.17.149  Bcast:10.24.17.255  Mask:255.255.255.0
          inet6 addr: fe80::2d0:b7ff:fe53:89c3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1107704 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2653820 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:390009908 (371.9 MiB)  TX bytes:809006934 (771.5 MiB)

eth1      Link encap:Ethernet  HWaddr 00:0E:0C:21:83:97
          inet addr:192.168.0.162  Bcast:10.24.17.255  Mask:255.255.255.0
          inet6 addr: fe80::20e:cff:fe21:8397/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1538726 errors:0 dropped:0 overruns:0 frame:0
          TX packets:356 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:341051195 (325.2 MiB)  TX bytes:22862 (22.3 KiB)
          Base address:0x5cc0 Memory:fbfe0000-fc000000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:3865 errors:0 dropped:0 overruns:0 frame:0
```

2 Benutzen Sie das ethtool-Kommando, um zwei NICs für das Management-LAN zu finden. Geben Sie das Kommando für jede der in Schritt 1 aufgeführten Schnittstellen in der unten wiedergegebenen Form ein.
Die NICs des Management-LANs haben die Bus-Informationen (SEG:BUS:GERAET.FUNK-Nummer) 0000:01:08.0 und 0000:01:00.0.
Kommandosyntax:

```
/sbin/ethtool –i <interface-name>
```

Beispiel: Die Ergebnisse der drei Kommandoaufrufe zeigen, dass den NICs des Management-LANs die beiden Ethernet-Schnittstellen eth0 und eth1 zugeordnet sind.

```
# /sbin/ethtool -i eth0
     driver: e100
     version: 3.0.27-k2-NAPI
     firmware-version: N/A
     bus-info: 0000:01:00.0 (Entspricht einer NIC für das Management-LAN)

# /sbin/ethtool -i eth1
     driver: e100
     version: 3.0.27-k2-NAPI
     firmware-version: N/A
     bus-info: 0000:01:08.0(Entspricht einer NIC für das Management-LAN)
```

(2) Zwei NICs für ein redundantes Management-LAN einrichten

Um das Management-LAN zu duplizieren, aktivieren Sie die beiden NICs für das Management-LAN in der Partition. Die Duplizierungssoftware (für LAN-Duplizierungen) überträgt den Datenstrom über die entsprechende Übertragungsleitung unter Berücksichtigung des Leitungsstatus und erreicht somit eine Redundanz. Wenn Sie eine Duplizierung festlegen, wird eine virtuelle Schnittstelle generiert, so dass die beiden NICs logisch wie eine NIC funktionieren. Der PSA und andere TCP/IP-Anwendungen verwenden die IP-Adresse der virtuellen Schnittstelle als lokale IP-Adresse des Systems, um mit dem entfernten System zu kommunizieren, ohne eine redundante physikalische Konfiguration berücksichtigen zu müssen.

Die Duplizierung kann über Bonding oder mit PRIMECLUSTER GLS durchgeführt werden. In beiden Fällen wird die Übertragungsleitung zum externen Switch überwacht und im Fehlerfall zur anderen Leitung umgeschaltet.

Wie aus Abbildung 4.1 hervorgeht, wird die Übertragungsleitung von der Partition zum externen Switch dupliziert, indem die Datenwege zum externe Switch, der an die Benutzerports der MMBs angeschlossen ist, mit in die Überwachung eingeschlossen werden.

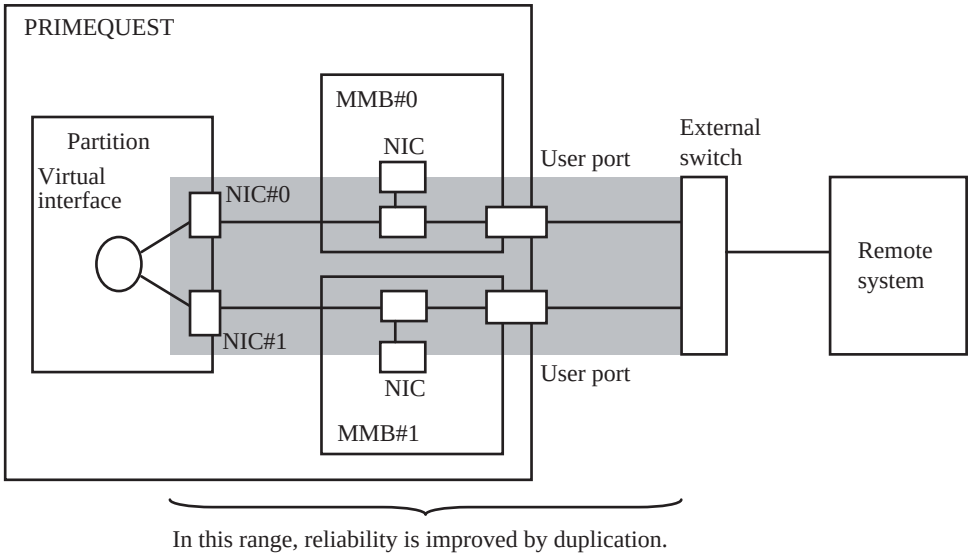


Abbildung 4.1 Konzept eines redundanten PRIMEQUEST-Management-LANs

Zusätzlich kann die Verfügbarkeit erhöht werden, indem der externe Switch und die Datenwege zum entfernten System redundant ausgeführt werden, wie in Abbildung 4.2 gezeigt wird. Die entsprechenden Einstellungen müssen auf dem entfernten System gemacht werden.

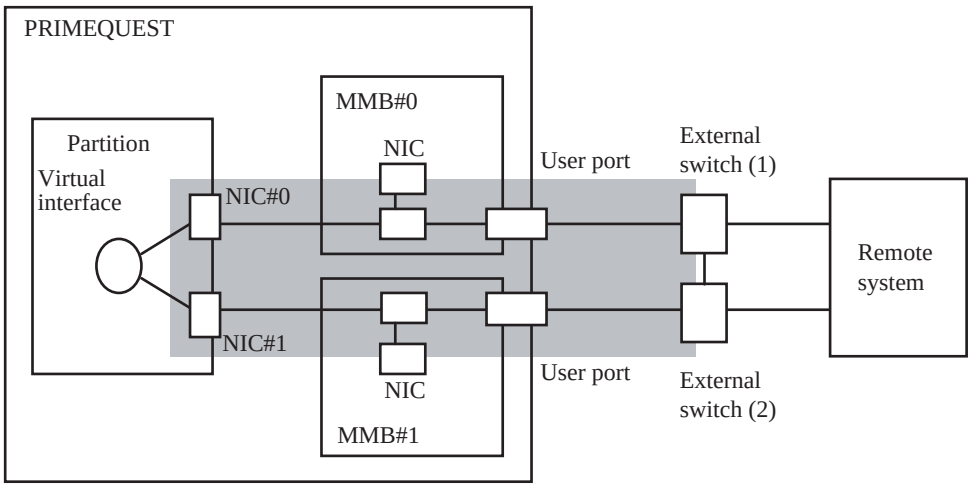


Abbildung 4.2 Konzept eines redundanten PRIMEQUEST-Management-LANs (Konfiguration mit erhöhter Verfügbarkeit)

- Bonding

  Hinweis: Ändern Sie die VLAN-Einstellung für den Management-LAN-Hub des MMB in „VLAN Mode“. (Näheres finden Sie unter 2.2.4.5, „Einen Management-LAN-Hub einrichten“.)

1 Fügen Sie in die Datei /etc/modprobe.conf die unten angegebenen Zeilen ein. Weisen Sie der Bonding-Schnittstelle einen Namen zu (bondN, wobei N eine Zahl in aufsteigender Folge ist).

```
# vi /etc/modprobe.conf

alias <management LAN NIC interface name 1> e100
alias <management LAN NIC interface name 2> e100
Folgende Zeilen hinzufügen:
alias <Bonding interface name> bonding
options <Bonding interface name> max_bonds=N+1          //note
options <Bonding interface name> mode=1
options <Bonding interface name> arp_interval=1000
options <Bonding interface name> arp_ip_target=<external switch IP address>
```

Hinweise:

1. Wenn mehrere Bonding-Schnittstellen benötigt werden, geben Sie die gewünschte Anzahl Schnittstellen an, indem Sie „max_bonds“ in den bond0-Optionen mit angeben. Die Standardwert des Parameters ist „max_bonds=1“.
2. Für die in Abbildung 4.1 dargestellte Konfiguration muss eine IP-Adresse angegeben werden. Für die in Abbildung 4.2 dargestellte Konfiguration sind zwei IP-Adressen erforderlich.

```
options <Bonding interface name> arp_ip_target=< external switch(1) IP address>,
< external switch(2) IP address>
```

Beispiel 1: Bonding-Schnittstelle anlegen

Bei der folgenden Beispieldatei /etc/modprobe.conf wird davon ausgegangen, dass eth0 und eth1 die Schnittstellen des Management-LANs sind. Die IP-Adresse des externen Switch 1 lautet in der Konfiguration aus Abbildung 4.2 10.20.100.10 und die IP-Adresse des externen Switch (2) lautet 10.20.100.11.

```
alias eth0 e100
alias eth1 e100
alias bond0 bonding
options bond0 mode=1
options bond0 arp_interval=1000
options bond0 arp_ip_target=10.20.100.10, 10.20.100.11
```

Beispiel 2: Bonding-Schnittstelle hinzufügen

In der folgenden Beispieldatei /etc/modprobe.conf wird davon ausgegangen, dass eth0 und eth1 die Schnittstellen des Management-LANs sind. Die IP-Adresse des externen Switch 1 lautet in der Konfiguration aus Abbildung 4.2 10.20.100.10 und die IP-Adresse des externen Switch (2) lautet 10.20.100.11.

```
alias bond0 bonding
options bond0 mode=0
options bond0 miimon=100
Folgende Zeilen hier einfügen:
options bond0 max_bonds=2
alias bond1 bonding
options bond1 mode=1
options bond1 arp_interval=1000
options bond1 arp_ip_target=10.20.100.10, 10.20.100.11
```

2 Ändern Sie die ifcfg-Datei der betreffenden Schnittstelle unter /etc/sysconfig/. Wenn die Datei nicht existiert, legen Sie sie an.

Hinweis: Wenn für das Management-LAN bereits Netzwerkeinstellungen vorgenommen wurden, weisen Sie die IP-Adressen für das Bonding in der ifcfg-Datei zu. Ändern Sie die ifcfg-Datei gemäß der Beschreibung einer Duplizierung des Management-LAN, die weiter unten in diesem Abschnitt enthalten ist.

- NIC-Schnittstelle 0 des Management-LANs: ifcfg-<interface name 1>
  Beispiel ifcfg-eth0
- NIC-Schnittstelle 1 des Management-LANs: ifcfg-<interface name 2>
  Beispiel ifcfg-eth1
- Bonding-Schnittstelle: ifcfg-<Bonding interface name>
  Beispiel ifcfg-bond0

Zur Einrichtung der ifcfg-Datei für die NIC-Schnittstelle des Management-LANs ist eine Hardware-Adresse erforderlich.

Führen Sie das Kommando ifconfig aus, um die Adresse zu bestätigen.

Kommandosyntax:

```
/sbin/ifconfig –a
```

Beispiel: Die Hardware-Adresse der Schnittstelle eth0 lautet 00:D0:B7:53:89:C3.

```
# /sbin/ifconfig –a
eth0      Link encap:Ethernet  HWaddr 00:D0:B7:53:89:C3
          inet addr:10.24.17.149  Bcast:10.24.17.255  Mask:255.255.255.0
          inet6 addr: fe80::2d0:b7ff:fe53:89c3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1107704 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2653820 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:390009908 (371.9 MiB)  TX bytes:809006934 (771.5 MiB)
```

Erstellen oder ändern Sie die ifcfg-Datei jeder Schnittstelle.

- ifcfg-Datei für die NIC-Schnittstelle des Management-LANs ändern

```
# vi /etc/sysconfig/network-scripts/ifcfg-<NIC interface name>

Folgende Zeilen ändern oder einfügen (beliebige Reihenfolge)
DEVICE=<NIC interface name>
BOOTPROTO=none
HWADDR=<hardware address>
ONBOOT=yes
MASTER=<Bonding interface name>
SLAVE=yes
```

- ifcfg-Datei für die Bonding-Schnittstelle ändern

```
# vi /etc/sysconfig/network-scripts/ifcfg-<Bonding interface name>

Folgende Zeilen ändern oder einfügen (beliebige Reihenfolge).
DEVICE=<Bonding interface name>
BOOTPROTO=static
ONBOOT=yes
BROADCAST=<management LAN BROADCAST address>
IPADDR=<management LAN IP address>
NETMASK=<management LAN subnet mask>
```

Beispiel: In den folgenden Beispielen der ifcfg-Datei, wird davon ausgegangen, dass eth0 und eth1 die Schnittstellen des Management-LANs sind und bond0 die Bonding-Schnittstelle ist.

- ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=none
HWADDR=00:04:23:AB:94:5E
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

- ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=none
HWADDR=00:04:23:AB:94:5F
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

- ifcfg-bond0

```
DEVICE=bond0
BOOTPROTO=static
ONBOOT=yes
BROADCAST=192.168.0.255
IPADDR=192.168.0.1
NETMASK=255.255.255.0
```

Starten Sie den Netzwerkdienst neu, um die Bonding-Schnittstelle zu aktivieren.

Kommandosyntax:

```
/sbin/service network restart
```

Hinweis: Der PSA muss neu gestartet werden, damit die NIC-Einstellungen für das Management-LAN in Kraft treten.

Kommandosyntax:

```
/sbin/service y30FJSVpsa stop
/sbin/service y30FJSVpsa start
```

- PRIMECLUSTER GLS

  Eine Beschreibung der für die Duplizierung des Management-LANs mit PRIMECLUSTER GLS erforderlichen Einstellungen finden Sie in den Handbüchern für PRIMECLUSTER GLS.

  Nur die „NIC Switching-Methode“ kann für die Duplizierung des Management-LANs angewendet werden.

  Derzeit müssen die externen Switches am Benutzerport des MMB in Abbildung 4.1 und Abbildung 4.2 als überwachte Hubs eingerichtet werden.

  Hinweis: Wenn für das Management-LAN bereits ein Netzwerk konfiguriert wurde, benutzen Sie für PRIMECLUSTER GLS die IP-Adresse aus der ifcfg-Datei und folgen Sie bei der Konfiguration der Duplikation den Anweisungen des PRIMECLUSTER GLS Handbuchs.

  Wenn Sie die Einstellungen für die Duplikation über GLS gemacht haben, starten Sie den Netzwerkdienst und den PSA neu.

  Kommandosyntax:

```
/sbin/service y30FJSVpsa stop
/sbin/service y30FJSVpsa start
```

4.2.2 Einstellungen für SELinux überprüfen

Überprüfen Sie, ob in dem Betriebssystem (Red Hat Linux) der Partition, in der Sie den PSA installieren, SELinux aktiviert ist und deaktivieren Sie SELinux in dem Fall.

PRIMEQUEST wird bei deaktivierten SELinux-Funktionen betrieben.

Gehen Sie wie folgt vor, um sicherzustellen, dass SELinux deaktiviert sind. Wenn SELinux aktiviert sind, deaktivieren Sie es in der Datei /etc/selinux/config.

- Einstellung überprüfen

```
#cd /etc/selinux/
#more config

.........
SELINUX=disabled
.........
```

- Einstellung ändern

```
# vi /etc/selinux/config
Change the following definition:
.........
SELINUX=disabled
```

4.2.3 Firewall überprüfen (Ports freigeben)

Wenn die Ports der Partition nicht freigegeben wurden, als die Firewall-Einstellungen gemacht wurden, geben Sie nun die für den PSA-Betrieb erforderlichen Ports des Management-LANs frei. Geben Sie insbesondere die folgenden Ports frei:

- snmp-Port : udp / snmp oder 161
- snmptrap-Port : udp / snmptrap oder 162 (*1) (zur physikalischen IP-Adresse des MMBs (beide Systeme))
- web-mmb Kommunikationsport: tcp / fj-webgate oder 24450 (*2) (zur virtuellen IP-Adresse des MMBs)
- rmcp+-Port : udp/7000 bis 7100 (*1) (zur physikalischen IP-Adresse des MMBs (beide Systeme))
- snmp-Port des lokalen Rechners: udp/1025-65535
- psa-mmb Kommunikationsport: Port 5000 für tcp/MMB (*3) (zur virtuellen IP-Adresse des MMBs) icmp/icmp-Typ0, icmp-Typ8 (zur virtuellen IP-Adresse des MMBs)

*1 Geben Sie den Port nur frei, wenn eine PCL-Verbindung verwendet wird. Überprüfen Sie die Firewall-Einstellungen mit dem Kommando iptables.

*2 web-mmb Kommunikationsport

*3 Dies ist der Kommunikationsport 5000 für MMB.
Da die Partition in dieser Kommunikation als Client fungiert, ist die Portnummer auf Partition-Seite undefiniert. (Eine beliebige Nummer von tcp/1025 bis 65535 wird für einen Port ausgewählt.)
Wie das folgende Beispiel zeigt, ist darüber hinaus keine Einstellung für Portnummer 5000 verlangt, wenn der Verbindungsaufbau von der Partition aus möglich ist oder wenn die Kommunikation für die Verbindung mit der eingerichteten Partition möglich ist.

(Beispiel) iptables -A OUTPUT -m state --state NEW,ESTABLISH -j ACCEPT
iptables -A INPUT -m state --state ESTABLISH -j ACCEPT

Kommandosyntax:

```
/sbin/iptables –L
```

Geben Sie einen Port mithilfe des Kommandos iptables oder eines anderen Kommandos frei. Näheres finden Sie in den Manual Pages des Betriebssystems.

Kommandosyntax:

```
/usr/bin/man iptables
```

4.2.4 FJSVfefpcl installieren

Anm.: FJSVfefpcl wird nur in Japan unterstützt.

4.2.5 Ziel für Partition-Traps festlegen

Hinweise:

- Machen Sie diese Einstellung nur, wenn sie erforderlich ist.
- Die Einstellung ist erforderlich, wenn Partitionen mit einer Betriebsverwaltungssoftware verwaltet werden.

Das Ziel der SNMP-Traps einer Partition muss auf der Partition eingestellt werden. Fügen Sie das Ziel in die Datei snmpd.conf ein.

- Datei snmpd.conf modifizieren

```
# vi /etc/snmp/snmpd.conf

Folgende Zeilen für die SNMP-Version einfügen. Beliebige Reihenfolge.
trapsink HOST [COMMUNITY [PORT]]   # Trap-Einstellungen für SNMPv1
trap2sink HOST [COMMUNITY [PORT]] # Trap-Einstellungen für SNMPv2
trapsess SNMPCMD_ARGS HOST[:PORT] # Trap-Einstellungen für SNMPv3
```

In unserem Beispiel sind folgende Einstellungen erforderlich:

- SNMPv1/SNMPv2-Traps einstellen

```
trapsink HOST [COMMUNITY [PORT]]   # Trap-Einstellungen für SNMPv1
trap2sink HOST [COMMUNITY [PORT]] # Trap-Einstellungen für SNMPv2
```

Geben Sie den Host an, an den die Traps gesendet werden sollen.

- Bei dieser Einstellung wird eine Kaltstart-Trap übertragen, wenn snmpd gestartet wird. Wenn die Übertragung von SMNP-Traps von der Partition festgelegt wurde, dann wird auch im Falle einer fehlgeschlagenen Authentifizierung eine Trap übertragen.
- Indem Sie mehrere Zeilenpaare für trapsink und trap2sink in die Datei einfügen, können Sie für die Traps mehrere Ziele festlegen.
- Wenn COMMUNITY nicht festgelegt wurde, wird die Zeichenkette verwendet, die zuvor von der trapcommunity-Anweisung festgelegt wurde.
  Mit dem Kommando trapcommunity wird die Standardzeichenkette für die Übertragung von Traps festgelegt. Geben Sie bei Verwendung dieses Kommandos die String vor dem Zeilenpaar trapsink-trap2sink ein.

```
trapcommunity STRING                    #COMMUNITY-Name
```

- Wenn kein spezifischer Port angegeben wird, wird der Standardport für SNMP-Traps (162) benutzt.

Beispiel: Wenn Sie Traps mit dem Community-Name „public“ an den Port 162 des Managementsystem mit der IP-Adresse 192.168.0.162 senden wollen:

```
trapsink  192.168.0.162  public  162          ##Trap-Einstellung für SNMPv1
trap2sink  192.168.0.162  public  162         ##Trap-Einstellung für SNMPv2
```

● Trap-Einstellungen für SNMPv3

```
trapsess SNMPCMD_ARGS HOST[:PORT]    #Trap-Einstellung für SNMPv3
```

Geben Sie den Host an, an den die Traps gesendet werden sollen. Wenn kein spezifischer Port angegeben wird, wird der Standardport für SNMP-Traps (162) benutzt.

Die folgenden Optionen stehen für SNMPCMD_ARGS zur Verfügung:

-v version : SNMP-Version. Geben Sie für SNMPv3 eine 3 an.

-e engineID: Die oldEngineID aus der Datei /var/net-snmp/snmpd.conf des Trap-Senders.

-u secName: Das SNMPv3-Benutzerkonto. Dieselbe Einstellung wie beim Managementsystem ist erforderlich.

-l secLevel : Je nach Sicherheitsstufe der SNMPv3-Meldungen, eine der folgenden Optionen:

Tabelle 4.2 Sicherheitsstufen

Einstellung	Authentifizierung	Verschlüsselung
noAuthNoPriv	Nein	Nein
authNoPriv	Ja	Nein
authPriv	Ja	Ja

-a authProtocol: Legt MD5 oder SHA als verwendetes Protokoll für die Authentifizierung von SNMPv3-Meldungen fest. Bei SHA muss ein Paket mit dem installierten openssl erstellt werden. Diese Option ist gültig, wenn in der mit der Option -l festgelegten Sicherheitsstufe eine Authentifizierung enthalten ist. Wenn keine Authentifizierung enthalten ist, kann diese Option entfallen.

-A authPassword: Legt das Kennwort für die Authentifizierung fest (mindestens 8 Zeichen). Es muss sich um dasselbe Kennwort wie beim Managementsystem handeln. Diese Option gilt, wenn in der mit der Option -l festgelegten Sicherheitsstufe eine Authentifizierung enthalten ist. Wenn keine Authentifizierung enthalten ist, kann diese Option entfallen.

-x privProtocol: Legt das Verschlüsselungsverfahren für SNMPv3-Meldungen fest. Aktuell wird nur DES unterstützt. Diese Option gilt, wenn in der mit der Option -l festgelegten Sicherheitsstufe eine Verschlüsselung vorgesehen ist. Wenn keine Verschlüsselung vorgesehen ist, kann diese Option entfallen.

-X privPassword: Legt ein verschlüsseltes Kennwort fest (mindestens 8 Zeichen). Es muss sich um dasselbe Kennwort wie beim Managementsystem handeln. Diese Option gilt, wenn in der mit der Option -l festgelegten Sicherheitsstufe eine Verschlüsselung vorgesehen ist. Wenn keine Verschlüsselung vorgesehen ist, kann diese Option entfallen.

Beispiel: SNMPv3-Traps sollen mit dem Benutzerkonto „PRIMEQUEST“ mit Authentifizierung und Verschlüsselung an den Port 162 des Managementsystems mit der IP-Adresse 192.168.0.162 gesendet werden:

```
trapsess -v 3 -e 0x800007e58026577a9f421950a4 -u PRIMEQUEST -l authPriv -a
MD5 -A 00000000
-x DES -X 11111111 192.168.0.162:162      ##SNMPv3 Trap-Einstellung
```

Wenn das Ziel für die Übertragung der Traps festgelegt ist, starten Sie snmpd mit dem folgenden Kommando neu:

```
#/etc/rc.d/init.d/snmpd restart
```

Aktivieren Sie PSA, nachdem snmpd reaktiviert wurde.

```
#/sbin/service y30FJSVpsa stop
#/sbin/service y30FJSVpsa start
```

Einstellungen des Trap-Ziels überprüfen

Verwenden Sie die standardmäßige net-snmp-Trap, mit der snmpd neu gestartet werden würde, um die Einstellungen für das Trap-Ziel zu überprüfen. Überprüfen Sie, ob die Trap ordnungsgemäß am Ziel empfangen wird.

Anm.: Am Trap-Ziel muss eine entsprechende Anwendung aktiviert sein, damit die Traps empfangen werden können.

Starten Sie snmpd neu, indem Sie auf dem Ausgangssystem das folgende Kommando ausführen:

```
# /etc/rc.d/init.d/snmpd restart
```

Die Trap-Anwendung auf dem Zielrechner erhält die Standardmeldung „ColdStart“.

Handelt es sich bei dem Zielrechner beispielsweise um einen Linux-Rechner, wird die folgende Meldung in die Datei syslog geschrieben, wenn snmptrapd eine Trap erhält. Das zeigt, dass das Zielgerät Traps ordnungsgemäß empfängt.

Aug 17 12:00:53 shaka snmptrapd[2600]: 2005-08-17 12:00:53 pq-server.fujitsu.com [192.168.0.162] (via 192.168.0.162) TRAP, SNMP v1, community public NET-SNMP-MIB::netSnmpAgentOIDs.10 Cold Start Trap (0) Uptime: 0:00:00.17

4.2.6 Ziel für Traps und E-Mails über MMB festlegen

Hinweise:

- Machen Sie diese Einstellung nur, wenn sie erforderlich ist.
- Die Einstellung ist erforderlich, wenn Partitionen mit einer Betriebsverwaltungssoftware (z.B. Systemwalker) verwaltet werden.

Das Ziel für Traps und E-Mails kann mit der MMB Web-UI eingestellt werden.

Näheres über das MMB Trap-Ziel finden Sie in Abschnitt 5.1.2, „SNMP einrichten“. Näheres über das E-Mail-Ziel finden Sie in Abschnitt 2.2.3.5, „SMTP-Einstellungen“.

4.2.7 Sonstige Einstellungen

Anm.: Machen Sie diese Einstellungen nur, wenn sie erforderlich sind.

- Diese Einstellung ist erforderlich, wenn ein repliziertes Laufwerk eingesetzt wird Sie können eine neue Partition erstellen, indem Sie ein Laufwerk einer Partition desselben Schranks kopieren. In diesem Fall muss die EngineID von SNMPv3 geändert werden, die vom PSA für die interne Kommunikation verwendet wird. Die EngineID kann mit root-Berechtigung wie folgt geändert werden:

1 Überprüfen Sie mit dem Kommando ps, ob der PSA aktiv ist.

Kommandosyntax:

```
ps ax | grep psa
```

Beispiel: Wenn unter /opt/FJSVpsa/bin/ die folgenden Prozesse aufgeführt werden, ist der PSA aktiv.

```
# ps ax | grep psa
 4562 ?        S      0:00 /opt/FJSVpsa/bin/pm -o 70 /etc/opt/FJSVpsa/
global/pmpsa.conf
 4563 ?        S      0:18 /opt/FJSVpsa/bin/loggetd -p /
 4564 ?        S      0:06 /opt/FJSVpsa/bin/sisp -p /
 4565 ?        S      0:00 /opt/FJSVpsa/bin/mmbm -p /
 4566 ?        S      0:01 /opt/FJSVpsa/bin/mmbs -p /
 4567 ?        S      0:02 /opt/FJSVpsa/bin/fs -p /
 4568 ?        S      0:00 /opt/FJSVpsa/bin/ciipmi -p /
 4569 ?        S      7:40 /opt/FJSVpsa/bin/cilog -p /
 4570 ?        S      8:47 /opt/FJSVpsa/bin/cios -p /
        .
        .
 4578 ?        S      0:00 /opt/FJSVpsa/bin/cisalchild 1 /
 4819 ?        Sl     0:00 /opt/FJSVpsa/bin/webgate -p /
 21670 pts/5   S+     0:00 grep psa
```

2 Wenn der PSA aktiv ist, deaktivieren Sie ihn mit dem Kommando stop.

Kommandosyntax:

```
/sbin/service y30FJSVpsa stop
```

3 Führen Sie das Kommando ps aus, um zu überprüfen, ob snmpd aktiv ist.

Kommandosyntax:

```
ps ax | grep snmpd
```

Beispiel: snmpd ist aktiv, wenn /usr/sbin/snmpd angezeigt wird.

```
# ps ax | grep snmpd
32611 ?        S      0:04 /usr/sbin/snmpd -Lsd -Lf /dev/null -p /var/run/
snmpd -a
```

4 Wenn snmpd aktiv ist, führen Sie das Kommando service aus, um snmpd zu deaktivieren.

Kommandosyntax:

```
/sbin/service snmpd stop
```

5 Ändern Sie den Wert für oldEngineID in der Datei /var/net-snmp/snmpd.conf.

Anm.: Sie können einen beliebigen Wert aus max. 34 Hexadezimalzahlen wählen. Der Wert muss innerhalb der Partitionen eines Schrankes einmalig sein.

Beispiel: Der Wert für oldEngineID wird in 0x19760523 geändert.

```
#vi /var/net-snmp/snmpd.conf
oldEngineID 0x19760523
```

6 Führen Sie das Kommando service aus, um snmpd zu aktivieren.

Kommandosyntax:

```
/sbin/service snmpd start
```

7 Wechseln Sie in das Verzeichnis /opt/FJSVpsa/sh/, um das Kennwort für snmpv3 für die interne Kommunikation des PSA neu zu generieren.

Kommandosyntax:

```
cd /opt/FJSVpsa/sh/
```

8 Führen Sie in dem genannten Verzeichnis das Kommando snmpsetup.sh aus. Damit wird das snmpv3-Kennwort automatisch generiert, das für die interne Kommunikation des PSA verwendet wird.

Kommandosyntax:

```
./snmpsetup.sh install
```

9 Starten Sie den PSA.

Kommandosyntax:

```
/sbin/service y30FJSVpsa start
```

4.2.8 PSA-Update installieren

Führen Sie die folgenden Kommandos in der angegebenen Reihenfolge aus, deaktivieren Sie den PSA und installieren Sie das neue PSA-Paket.

Hinweis: Ist PEXU gemountet, verwenden Sie PSA ab 1.10.

Kommandosyntax:

Update von PSA-1.2.X-X oder höher

```
/sbin/service y30FJSVpsa stop
/bin/rpm -Uvh FJSVpsa-X.X.X-X.ia64.rpm
/sbin/service y30FJSVpsa start
```

Update von PSA-1.1.X-X

```
/sbin/service y30FJSVpsa stop
/bin/rpm -Uvh FJSVpsa-X.X.X-X.ia64.rpm
/sbin/service y10FJSVpsa start
/sbin/service y30FJSVpsa start
```

* X.X.X-X ist die PSA-Versionsnummer.

[Beginn des Zusatzes gemäß Manual Errata 2009/02/24]

Beim PSA-Update automatisch vorgenommene Einstellungen

Die folgenden Modifikationen, die für den PSA-Betrieb erforderlich sind, werden beim PSA-Update automatisch wirksam:

- Korrektur der Gerätetypen in der Datei scsi.agent (von PSA1.16.1-xRHEL4 oder früher bis PSA1.16.2-xRHEL4 oder später)
- Löschung der Einstellungen in der Datei crontab (wenn PSA zwischen PSA1.3.x-xRHEL4 und PSA1.6.x-xRHEL4 atualisiert wird auf PSA1.7.x-xRHEL4 oder später)
- Änderung der Boot-Option snmptrapd (PSA1.19.1-x oder später)

[Ende des Zusatzes gemäß Manual Errata 2009/02/24]

4.2.9 SIRMS-Update installieren

Installieren Sie die Updates für die beiden SIRMS-Pakete mit den folgenden Kommandos.

Kommandosyntax:

```
/bin/rpm -Uvh sirms-X.X.X-X.ia64.rpm
/bin/rpm -Uvh FJSVsoftmsg-X.X.X-X.ia64.rpm
```

* X.X.X-X ist die Versionsnummer.

4.2.10 PSA deinstallieren

Führen Sie die folgenden Kommandos in der angegebenen Reihenfolge aus, deaktivieren Sie den PSA und deinstallieren Sie das PSA-Paket.

Kommandosyntax:

```
/sbin/service y30FJSVpsa stop
/bin/rpm -e FJSVpsa
```

[Beginn des Zusatzes gemäß Manual Errata 2009/02/24]

Bei der Deinstalltion automatisch vorgenommene Einstellungen

Die folgenden Modifikationen werden bei der PSA-Deinstallation automatisch wirksam:

- Löschen der Einstellungen in der Datei syslog.conf
- Löschen der Einstellungen in der Datei snmpd.conf
- Löschen der Einstellungen in der Datei snmptrapd.conf
- Aktivierung der automatischen Starteinstellungen von salinfo oder salinfo_decode
- Aktivierung der automatischen Starteinstellungen von smartd
- Löschen der Einstellungen in der Datei services
- Löschen der Einstellungen in der Datei crontab file (PSA1.3.x-xRHEL4 bis PSA1.6.x-xRHEL4)
- Ändern der Boot-Option snmptrapd

[Ende des Zusatzes gemäß Manual Errata 2009/02/24]

4.2.11 SIRMS deinstallieren

Deinstallieren Sie die beiden SIRMS-Paket mit den folgenden Kommandos.

Kommandosyntax:

```
/bin/rpm -e sirms
/bin/rpm -e FJSVsoftmsg
```

Hinweis: SIRMS sammelt Software-Konfigurationsdaten für REMCS*. Die Funktion muss zusammenmit dem PSA installiert werden, sie muss jedoch nicht installiert werden, wenn Sie eine Batch-Installation mit dem PRIMEQUEST Installationstool oder dem Installer für Software-Bundle-Packages vornehmen.

*: wird von Fujitsu Technology Solutions nicht unterstützt

4.3 PSA installieren (Linux: Red Hat) (PRIMEQUEST 520A*/520/420)

In diesem Abschnitt werden die Punkte beschrieben, die vor Installation des PSA überprüft werden müssen.

Obligatorische Aufgaben:

- Einstellungen des Management-LANs überprüfen (→ 4.3.1)
- Einstellungen für SELinux überprüfen (→ 4.3.2)
- Firewall überprüfen (Ports freigeben) (→ 4.3.3)
- FJSVfefpcl installieren (→ 4.3.4)

Optionale Aufgaben:

- Ziel für Partition-Traps festlegen (→ 4.3.5)
- Ziel für Traps und E-Mails über MMB festlegen (→ 4.3.6)
- Sonstige Einstellungen (→ 4.3.7)

Anm.:

- Benutzen Sie das PRIMEQUEST Installation Support Tool, den Installer für Software-Bundle-Packages oder SystemcastWizard Lite, um den PSA zu installieren. Wie Sie den PSA manuell installieren können, ist in Kapitel 4 „Manual PSA Installation“ im Handbuch *PRIMEQUEST 500A/500/400 Series Reference Manual: Tools/Operation Information* (U41757-J-Z816-x-76/C122-E074EN) beschrieben.
  Das PRIMEQUEST Installation Support Tool ist im *PRIMEQUEST Installation Support Tool User's Guide (Red Hat)* (C122-E005EN) beschrieben.
  Einzelheiten über den Installer für Software-Bundle-Packages finden Sie im *PRIMEQUEST Bundled-Software Package Installer User's Guide* (C122-E006EN).
  Näheres über SystemcastWizard Lite finden Sie im *PRIMEQUEST SystemcastWizard Lite User's Guide* (C122-E010EN).
- Während der Installation des PSA werden die folgenden für den Betrieb erforderlichen Modifikationen automatisch durchgeführt:
  - Hinzufügen ~~**von**~~ **der** Einstellungen in der **Datei** syslog.conf
  - Hinzufügen ~~**von**~~ **der** Einstellungen in der **Datei** snmpd.conf

*: wird von Fujitsu Technology Solutions nicht unterstützt

- ~~**Einrichten**~~ **Hinzufügen der Einstellungen in** der Datei snmptrapd.conf
- Deaktivierung der automatischen Starteinstellungen von salinfo oder salinfo_decode (*1)
- Deaktivierung der automatischen Starteinstellungen von smartd (*1)
- Einfügen der Beschreibung in die Datei services (*2)
- ~~**Korrekturen in scsi.agent (*3)**~~
- **Korrektur der Gerätetypen in der Datei scsi.agent (PSA1.16.2-xRHEL4 oder später) (*3)**
- **Hinzufügen der Einstellungen in der Datei crontab (PSA1.3.x-xRHEL4 bis PSA1.6.x-xRHEL4)**
- **Änderung der Boot-Option snmptrapd**

*1 Diese automatischen Starteinstellungen sind wegen Konflikten mit einigen PSA-Funktionen deaktiviert.

*2 Hinzugefügter Port:
Es wird nicht überprüft, ob Portnummern doppelt vorhanden sind, wenn ~~**weitere Daten**~~ **die Einstellungen** in die Dienstedatei fj-webgate (24450) eingefügt werden. Führen Sie eventuell notwendige Änderungen durch.

***3 Korrekturen werden nur unter RHEL-AS4 (IPF) vorgenommen.**

[Korrekturen (halbfett ausgezeichnet) gemäß Handbuch-Errata 2008/12/18 und 2009/02/24]

4.3.1 Einstellungen des Management-LANs überprüfen

In diesem Abschnitt wird beschrieben, wie Sie die Einstellungen des Management-LANs überprüfen können.
Damit der PSA über das Management-LAN mit dem MMB kommunizieren kann, muss die mit dem Management-LAN verbundene NIC (Network Interface Card) aktiv sein.

(1) Einstellungen für die NIC des Management-LANs überprüfen

Führen Sie das folgende Kommando aus, um den Namen der Schnittstelle zu überprüfen, der dem NIC des Management-LANs zugewiesen ist.

1 Geben Sie das Kommando ifconfig ein, um die vom System erkannten Netzwerkschnittstellen aufzulisten und den betreffenden Schnittstellennamen zu bestätigen.
Kommandosyntax:

```
/sbin/ifconfig –a
```

Beispiel: Die Schnittstellen heißen eth0, eth1 und lo.

```
# /sbin/ifconfig –a
eth0      Link encap:Ethernet  HWaddr 00:D0:B7:53:89:C3
          inet addr:10.24.17.149  Bcast:10.24.17.255  Mask:255.255.255.0
          inet6 addr: fe80::2d0:b7ff:fe53:89c3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1107704 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2653820 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:390009908 (371.9 MiB)  TX bytes:809006934 (771.5 MiB)

eth1      Link encap:Ethernet  HWaddr 00:0E:0C:21:83:97
          inet addr:192.168.0.162  Bcast:10.24.17.255  Mask:255.255.255.0
          inet6 addr: fe80::20e:cff:fe21:8397/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1538726 errors:0 dropped:0 overruns:0 frame:0
          TX packets:356 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:341051195 (325.2 MiB)  TX bytes:22862 (22.3 KiB)
          Base address:0x5cc0 Memory:fbfe0000-fc000000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:3865 errors:0 dropped:0 overruns:0 frame:0
```

2 Benutzen Sie das ethtool-Kommando, um einen NIC für das Management-LAN zu finden. Geben Sie das Kommando für jede der in Schritt 1 aufgeführten Schnittstellen in der unten wiedergegebenen Form ein.
Die NICs des Management-LANs haben die Bus-Informationen (SEG:BUS:GERAET.FUNK-Nummer) 0000:01:08.0 und 0000:01:00.0.
Kommandosyntax:

```
/sbin/ethtool –i <schnittstellen-name>
```

Beispiel: Die Ergebnisse der drei Kommandoaufrufe zeigen, dass den NICs des Management-LANs die beiden Ethernet-Schnittstellen eth0 und eth1 zugeordnet sind.

```
# /sbin/ethtool -i eth0
     driver: e100
     version: 3.0.27-k2-NAPI
     firmware-version: N/A
     bus-info: 0000:01:08.0 (Entspricht einer NIC für das Management-LAN)
```

(2) NIC für das Management-LAN einstellen

1 Ändern Sie die ifcfg-Datei, damit sie der relevanten Schnittstelle unter /etc/sysconfig/ in den Netzwerkskripts entspricht. Legen Sie die Datei an, wenn sie noch nicht existiert.

- NIC-Schnittstelle des Management-LAN: ifcfg-<Schnittstellenname> Beispiel: ifcfg-eth0

Für die Einstellung der ifcfg-Datei für die NIC-Schnittstelle des Management-LANs ist eine Hardware-Adresse erforderlich.
Benutzen Sie das Kommando ifconfig, um die Adresse zu überprüfen, wenn dies noch nicht geschehen ist.
Kommandosyntax:

```
/sbin/ifconfig –a
```

Beispiel: Die Hardware-Adresse der Schnittstelle eth0 lautet 00:D0:B7:53:89:C3.

```
# /sbin/ifconfig –a
eth0      Link encap:Ethernet  HWaddr 00:D0:B7:53:89:C3
          inet addr:10.24.17.149  Bcast:10.24.17.255  Mask:255.255.255.0
          inet6 addr: fe80::2d0:b7ff:fe53:89c3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1107704 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2653820 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:390009908 (371.9 MiB)  TX bytes:809006934 (771.5 MiB)
```

Erstellen oder ändern Sie die ifcfg-Datei jeder Schnittstelle.

- ifcfg-Datei für die NIC-Schnittstelle des Management-LANs ändern

```
# vi /etc/sysconfig/network-scripts/ifcfg-<NIC interface name>

Ändern oder ergänzen Sie die folgenden Zeilen wie folgt (die Reihenfolge der Zeilen ist beliebig).
DEVICE=<NIC-Schnittstellenname>
BOOTPROTO=none
HWADDR=<Hardware-Adresse>
ONBOOT=yes
MASTER=<Bonding-Schnittstellenname>
SLAVE=yes
BROADCAST=<Management-LAN BROADCAST-Adresse>
IPADDR=<Management-LAN IP-Adresse>
NETMASK=<Management-LAN Teilnetzmaske>
```

Beispiel: In dem folgenden Beispiel einer ifcfg-Datei, wird davon ausgegangen, dass die NIC-Schnittstellen des Management-LANs eth0 ist.

- ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=00:D0:B7:53:89:C3
ONBOOT=yes
BROADCAST=192.168.0.255
IPADDR=192.168.0.1
NETMASK=255.255.255.0
```

Starten Sie den Netzwerkdienst neu, um die Netzwerkschnittstelle zu aktivieren.

Kommandosyntax:

```
/sbin/service network restart
```

Der PSA muss neu gestartet werden, damit die NIC-Einstellungen für das Management-LAN in Kraft treten.

Kommandosyntax:

```
/sbin/service y30FJSVpsa stop
/sbin/service y30FJSVpsa start
```

4.3.2 Einstellungen für SELinux überprüfen

Überprüfen Sie, ob in dem Betriebssystem (Red Hat Linux) der Partition, in der Sie den PSA installieren, SELinux aktiviert ist und deaktivieren Sie SELinux in dem Fall.

PRIMEQUEST wird bei deaktivierten SELinux-Funktionen betrieben.

Gehen Sie wie folgt vor, um sicherzustellen, dass SELinux deaktiviert sind. Wenn SELinux aktiviert sind, deaktivieren Sie es in der Datei /etc/selinux/config.

- Einstellung überprüfen

```
#cd /etc/selinux/
#more config

.........
SELINUX=disabled
.........
```

- Einstellung ändern

```
# vi /etc/selinux/config
Change the following definition:
.........
SELINUX=disabled
```

4.3.3 Firewall überprüfen (Ports freigeben)

Wenn die Ports der Partition nicht freigegeben wurden, als die Firewall-Einstellungen gemacht wurden, geben Sie nun die für den PSA-Betrieb erforderlichen Ports des Management-LANs frei. Geben Sie insbesondere die folgenden Ports frei:

- snmp-Port : udp / snmp oder 161
- snmptrap-Port : udp / snmptrap oder 162 (*1)
  (zur IP-Adresse des MMBs)
- web-mmb Kommunikationsport: tcp / fj-webgate oder 24450 (*2)
  (zur IP-Adresse des MMBs)
- rmcp+-Port : udp/7000 bis 7100 (*1)
  (zur IP-Adresse des MMBs)
- snmp-Port des lokalen Rechners: udp/1025-65535
- psa-mmb Kommunikationsport: Port 5000 für tcp/MMB (*3)
  (zur virtuellen IP-Adresse des MMBs)
  icmp/icmp-Typ0, icmp-Typ8
  (zur virtuellen IP-Adresse des MMBs)

*1 Geben Sie den Port nur frei, wenn eine PCL-Verbindung verwendet wird. Überprüfen Sie die Firewall-Einstellungen mit dem Kommando iptables.

*2 web-mmb Kommunikationsport

*3 Dies ist der Kommunikationsport 5000 für MMB.
Da die Partition in dieser Kommunikation als Client fungiert, ist die Portnummer auf Partition-Seite undefiniert. (Eine beliebige Nummer von tcp/1025 bis 65535 wird für einen Port ausgewählt.)
Wie das folgende Beispiel zeigt, ist darüber hinaus keine Einstellung für Portnummer 5000 verlangt, wenn der Verbindungsaufbau von der Partition aus möglich ist oder wenn die Kommunikation für die Verbindung mit der eingerichteten Partition möglich ist.

(Beispiel) iptables -A OUTPUT -m state --state NEW,ESTABLISH -j ACCEPT
iptables -A INPUT -m state --state ESTABLISH -j ACCEPT

Kommandosyntax:

```
/sbin/iptables –L
```

Geben Sie einen Port mithilfe des Kommandos iptables oder eines anderen Kommandos frei. Näheres finden Sie in den Manual Pages des Betriebssystems.

Kommandosyntax:

```
/usr/bin/man iptables
```

4.3.4 FJSVfefpcl installieren

Anm.: FJSVfefpcl wird nur in Japan unterstützt.

4.3.5 Ziel für Partition-Traps festlegen

Hinweise:

- Machen Sie diese Einstellung nur, wenn sie erforderlich ist.
- Die Einstellung ist für die Verbindung zu einer Betriebsverwaltungssoftware erforderlich.

Das Ziel der SNMP-Traps einer Partition muss eingestellt werden. Fügen Sie das Ziel in die Datei snmpd.conf ein.

- Datei snmpd.conf modifizieren

```
# vi /etc/snmp/snmpd.conf

Folgende Zeilen für die SNMP-Version einfügen. Beliebige Reihenfolge.
trapsink HOST [COMMUNITY [PORT]]  # Trap-Einstellungen für SNMPv1
trap2sink HOST [COMMUNITY [PORT]] # Trap-Einstellungen für SNMPv2
trapsess SNMPCMD_ARGS HOST[:PORT] # Trap-Einstellungen für SNMPv3
```

In unserem Beispiel sind folgende Einstellungen erforderlich:

- SNMPv1/SNMPv2-Traps einstellen

```
trapsink HOST [COMMUNITY [PORT]]  # Trap-Einstellungen für SNMPv1
trap2sink HOST [COMMUNITY [PORT]] # Trap-Einstellungen für SNMPv2
```

Geben Sie den Host an, an den die Traps gesendet werden sollen.

- Bei dieser Einstellung wird eine Kaltstart-Trap übertragen, wenn snmpd gestartet wird. Wenn die Übertragung von SMNP-Traps von der Partition festgelegt wurde, dann wird auch im Falle einer fehlgeschlagenen Authentifizierung eine Trap übertragen.
- Indem Sie mehrere Zeilenpaare für trapsink und trap2sink in die Datei einfügen, können Sie für die Traps mehrere Ziele festlegen.
- Wenn COMMUNITY nicht festgelegt wurde, wird die Zeichenkette verwendet, die zuvor von der trapcommunity-Anweisung festgelegt wurde.
  Mit dem Kommando trapcommunity wird die Standardzeichenkette für die Übertragung von Traps festgelegt. Geben Sie bei Verwendung dieses Kommandos die String vor dem Zeilenpaar trapsink-trap2sink ein.

```
trapcommunity STRING                    #COMMUNITY-Name
```

- Wenn kein spezifischer Port angegeben wird, wird der Standardport für SNMP-Traps (162) benutzt.

Beispiel: Wenn Sie Traps mit dem Community-Name „public“ an den Port 162 des Managementsystem mit der IP-Adresse 192.168.0.162 senden wollen:

```
trapsink  192.168.0.162  public  162          ##Trap-Einstellung für SNMPv1
trap2sink  192.168.0.162  public  162         ##Trap-Einstellung für SNMPv2
```

● Trap-Einstellungen für SNMPv3

```
trapsess SNMPCMD_ARGS HOST[:PORT]    #Trap-Einstellung für SNMPv3
```

Geben Sie den Host an, an den die Traps gesendet werden sollen. Wenn kein spezifischer Port angegeben wird, wird der Standardport für SNMP-Traps (162) benutzt.

Die folgenden Optionen stehen für SNMPCMD_ARGS zur Verfügung:

-v version : SNMP-Version. Geben Sie für SNMPv3 eine 3 an.

-e engineID: Die oldEngineID aus der Datei /var/net-snmp/snmpd.conf des Trap-Senders.

-u secName: Das SNMPv3-Benutzerkonto. Dieselbe Einstellung wie beim Managementsystem ist erforderlich.

-l secLevel : Je nach Sicherheitsstufe der SNMPv3-Meldungen, eine der folgenden Optionen:

Tabelle 4.3 Sicherheitsstufen

Einstellung	Authentifizierung	Verschlüsselung
noAuthNoPriv	Nein	Nein
authNoPriv	Ja	Nein
authPriv	Ja	Ja

-a authProtocol: Legt MD5 oder SHA als verwendetes Protokoll für die Authentifizierung von SNMPv3-Meldungen fest. Bei SHA muss ein Paket mit dem installierten openssl erstellt werden. Diese Option ist gültig, wenn in der mit der Option -l festgelegten Sicherheitsstufe eine Authentifizierung enthalten ist. Wenn keine Authentifizierung enthalten ist, kann diese Option entfallen.

-A authPassword: Legt das Kennwort für die Authentifizierung fest (mindestens 8 Zeichen). Es muss sich um dasselbe Kennwort wie beim Managementsystem handeln. Diese Option gilt, wenn in der mit der Option -l festgelegten Sicherheitsstufe eine Authentifizierung enthalten ist. Wenn keine Authentifizierung enthalten ist, kann diese Option entfallen.

-x privProtocol: Legt das Verschlüsselungsverfahren für SNMPv3-Meldungen fest. Aktuell wird nur DES unterstützt. Diese Option gilt, wenn in der mit der Option -l festgelegten Sicherheitsstufe eine Verschlüsselung vorgesehen ist. Wenn keine Verschlüsselung vorgesehen ist, kann diese Option entfallen.

-X privPassword: Legt ein verschlüsseltes Kennwort fest (mindestens 8 Zeichen). Es muss sich um dasselbe Kennwort wie beim Managementsystem handeln. Diese Option gilt, wenn in der mit der Option -l festgelegten Sicherheitsstufe eine Verschlüsselung vorgesehen ist. Wenn keine Verschlüsselung vorgesehen ist, kann diese Option entfallen.

Beispiel: SNMPv3-Traps sollen mit dem Benutzerkonto „PRIMEQUEST“ mit Authentifizierung und Verschlüsselung an den Port 162 des Managementsystems mit der IP-Adresse 192.168.0.162 gesendet werden:

```
trapsess -v 3 -e 0x800007e58026577a9f421950a4 -u PRIMEQUEST -l authPriv -a
MD5 -A 00000000
-x DES -X 11111111 192.168.0.162:162      ##SNMPv3 Trap-Einstellung
```

Wenn das Ziel für die Übertragung der Traps festgelegt ist, starten Sie snmpd mit dem folgenden Kommando neu:

```
#/etc/rc.d/init.d/snmpd restart
```

Starten Sie PSA neu, nachdem der Neustart von snmpd beendet ist.

```
#/sbin/service y30FJSVpsa stop
#/sbin/service y30FJSVpsa start
```

Einstellungen des Trap-Ziels überprüfen

Verwenden Sie die standardmäßige net-snmp-Trap, mit der snmpd neu gestartet werden würde, um die Einstellungen für das Trap-Ziel zu überprüfen. Überprüfen Sie, ob die Trap ordnungsgemäß am Ziel empfangen wird.

Anm.: Am Trap-Ziel muss eine entsprechende Anwendung aktiviert sein, damit die Traps empfangen werden können.

Starten Sie snmpd neu, indem Sie auf dem Ausgangssystem das folgende Kommando ausführen:

```
# /etc/rc.d/init.d/snmpd restart
```

Die Trap-Anwendung auf dem Zielrechner erhält die Standardmeldung „ColdStart“.

Handelt es sich bei dem Zielrechner beispielsweise um einen Linux-Rechner, wird die folgende Meldung in die Datei syslog geschrieben, wenn snmptrapd eine Trap erhält. Das zeigt, dass das Zielgerät Traps ordnungsgemäß empfängt.

Aug 17 12:00:53 shaka snmptrapd[2600]: 2005-08-17 12:00:53 pq-server.fujitsu.com [192.168.0.162] (via 192.168.0.162) TRAP, SNMP v1, community public NET-SNMP-MIB::netSnmpAgentOIDs.10 Cold Start Trap (0) Uptime: 0:00:00.17

4.3.6 Ziel für Traps und E-Mails über MMB festlegen

Hinweise:

- Machen Sie diese Einstellung nur, wenn sie erforderlich ist.
- Die Einstellung ist für die Verbindung zu einer Betriebsverwaltungs-software erforderlich (z.B. Systemwalker).

Das Ziel für Traps und E-Mails kann mit der MMB Web-UI eingestellt werden.

Näheres über das MMB Trap-Ziel finden Sie in Abschnitt 5.1.2, „SNMP einrichten“. Näheres über das E-Mail-Ziel finden Sie in Abschnitt 2.2.3.5, „SMTP-Einstellungen“.

4.3.7 Sonstige Einstellungen

Anm.: Machen Sie diese Einstellungen nur, wenn sie erforderlich sind.

- Diese Einstellung ist erforderlich, wenn ein repliziertes Laufwerk eingesetzt wird Sie können eine neue Partition erstellen, indem Sie ein Laufwerk einer Partition desselben Schranks kopieren. In diesem Fall muss die EngingID von SNMPv3 geändert werden, die vom PSA für die interne Kommunikation verwendet wird. Die EngineID kann mit root-Berechtigung wie folgt geändert werden:

1 Überprüfen Sie mit dem Kommando ps, ob der PSA aktiv ist.

Kommandosyntax:

```
ps ax | grep psa
```

Beispiel: Wenn unter /opt/FJSVpsa/bin/ die folgenden Prozesse aufgeführt werden, ist der PSA aktiv.

```
# ps ax | grep psa
 4562 ?        S      0:00 /opt/FJSVpsa/bin/pm -o 70 /etc/opt/FJSVpsa/
global/pmpsa.conf
 4563 ?        S      0:18 /opt/FJSVpsa/bin/loggetd -p /
 4564 ?        S      0:06 /opt/FJSVpsa/bin/sisp -p /
 4565 ?        S      0:00 /opt/FJSVpsa/bin/mmbm -p /
 4566 ?        S      0:01 /opt/FJSVpsa/bin/mmbs -p /
 4567 ?        S      0:02 /opt/FJSVpsa/bin/fs -p /
 4568 ?        S      0:00 /opt/FJSVpsa/bin/ciipmi -p /
 4569 ?        S      7:40 /opt/FJSVpsa/bin/cilog -p /
 4570 ?        S      8:47 /opt/FJSVpsa/bin/cios -p /
       .
       .
 4578 ?        S      0:00 /opt/FJSVpsa/bin/cisalchild 1 /
 4819 ?        Sl     0:00 /opt/FJSVpsa/bin/webgate -p /
 21670 pts/5   S+     0:00 grep psa
```

2 Wenn der PSA aktiv ist, deaktivieren Sie ihm mit dem Kommando stop.

Kommandosyntax:

```
/sbin/service y30FJSVpsa stop
```

3 Führen Sie das Kommando ps aus, um zu überprüfen, ob snmpd aktiv ist.

Kommandosyntax:

```
ps ax | grep snmpd
```

Beispiel: snmpd ist aktiv, wenn /usr/sbin/snmpd angezeigt wird.

```
# ps ax | grep snmpd
32611 ?        S      0:04 /usr/sbin/snmpd -Lsd -Lf /dev/null -p /var/run/
snmpd -a
```

4 Wenn snmpd aktiv ist, führen Sie das Kommando service aus, um snmpd zu deaktivieren.

Kommandosyntax:

```
/sbin/service snmpd stop
```

5 Ändern Sie den Wert für oldEngineID in der Datei /var/net-snmp/snmpd.conf.

Anm.: Sie können einen beliebigen Wert aus max. 34 Hexadezimalzahlen wählen. Der Wert muss innerhalb der Partitionen eines Schrankes einmalig sein.

Beispiel: Der Wert für oldEngineID wird in 0x19760523 geändert.

```
#vi /var/net-snmp/snmpd.conf
oldEngineID 0x19760523
```

6 Führen Sie das Kommando service aus, um snmpd zu aktivieren.

Kommandosyntax:

```
/sbin/service snmpd start
```

7 Wechseln Sie in das Verzeichnis /opt/FJSVpsa/sh/, um das Kennwort für snmpv3 für die interne Kommunikation des PSA neu zu generieren.

Kommandosyntax:

```
cd /opt/FJSVpsa/sh/
```

8 Führen Sie in dem genannten Verzeichnis das Kommando snmpsetup.sh aus. Damit wird das snmpv3-Kennwort automatisch generiert, das für die interne Kommunikation des PSA verwendet wird.

Kommandosyntax:

```
./snmpsetup.sh install
```

9 Starten Sie den PSA.

Kommandosyntax:

```
/sbin/service y30FJSVpsa start
```

4.3.8 PSA-Update installieren

Führen Sie die folgenden Kommandos in der angegebenen Reihenfolge aus, deaktivieren Sie den PSA und installieren Sie das neu PSA-Paket.

Hinweis: Ist PEXU gemountet, verwenden Sie PSA ab Version 1.10.

Kommandosyntax:

```
/sbin/service y30FJSVpsa stop
/bin/rpm -Uvh FJSVpsa-X.X.X-X.ia64.rpm
/sbin/service y30FJSVpsa start
```

* X.X.X-X ist die PSA-Versionsnummer.

[Beginn des Zusatzes gemäß Manual Errata 2009/02/24]

Beim PSA-Update automatisch vorgenommene Einstellungen

Die folgenden Modifikationen, die für den PSA-Betrieb erforderlich sind, werden beim PSA-Update automatisch wirksam:

- Korrektur der Gerätetypen in der Datei scsi.agent (von PSA1.16.1-xRHEL4 oder früher bis PSA1.16.2-xRHEL4 oder später)

- Löschung der Einstellungen in der Datei crontab (wenn PSA zwischen PSA1.3.x-xRHEL4 und PSA1.6.x-xRHEL4 atualisiert wird auf PSA1.7.x-xRHEL4 oder später)
- Änderung der Boot-Option snmptrapd (PSA1.19.1-x oder später)

[Ende des Zusatzes gemäß Manual Errata 2009/02/24]

4.3.9 SIRMS-Update installieren

Installieren Sie die Updates für die beiden SIRMS-Pakete mit den folgenden Kommandos.

Kommandosyntax:

```
/bin/rpm -Uvh sirms-X.X.X-X.ia64.rpm
/bin/rpm -Uvh FJSVsoftmsg-X.X.X-X.ia64.rpm
```

* X.X.X-X ist die Versionsnummer.

4.3.10 PSA deinstallieren

Führen Sie die folgenden Kommandos in der angegebenen Reihenfolge aus, deaktivieren Sie den PSA und deinstallieren Sie das PSA-Paket.

Kommandosyntax:

```
/sbin/service y30FJSVpsa stop
/bin/rpm -e FJSVpsa
```

[Beginn des Zusatzes gemäß Manual Errata 2009/02/24]

Bei der Deinstalltion automatisch vorgenommene Einstellungen

Die folgenden Modifikationen werden bei der PSA-Deinstallation automatisch wirksam:

- Löschen der Einstellungen in der Datei syslog.conf
- Löschen der Einstellungen in der Datei snmpd.conf
- Löschen der Einstellungen in der Datei snmptrapd.conf
- Aktivierung der automatischen Starteinstellungen von salinfo oder salinfo_decode
- Aktivierung der automatischen Starteinstellungen von smartd
- Löschen der Einstellungen in der Datei services
- Löschen der Einstellungen in der Datei crontab file (PSA1.3.x-xRHEL4 bis PSA1.6.x-xRHEL4)
- Ändern der Boot-Option snmptrapd

[Ende des Zusatzes gemäß Manual Errata 2009/02/24]

4.3.11 SIRMS deinstallieren

Deinstallieren Sie die beiden SIRMS-Paket mit den folgenden Kommandos.

Kommandosyntax:

```
/bin/rpm -e sirms
/bin/rpm -e FJSVsoftmsg
```

Hinweis: SIRMS sammelt Software-Konfigurationsdaten für REMCS*. Die Funktion muss zusammenmit dem PSA installiert werden, sie muss jedoch nicht installiert werden, wenn Sie eine Batch-Installation mit dem PRIMEQUEST Installationstool oder dem Installer für Software-Bundle-Packages vornehmen.

*: wird von Fujitsu Technology Solutions nicht unterstützt

4.4 PSA installieren (Linux: SUSE) (PRIMEQUEST 500A/500/400-Modellreihe)

In diesem Abschnitt werden die Punkte beschrieben, die vor Installation des PSA überprüft werden müssen.

Obligatorische Aufgaben:

- Einstellungen des Management-LANs überprüfen (→ 4.4.1)
- Firewall überprüfen (Ports freigeben) (→ 4.4.4)

Optionale Aufgaben:

- Ziel für Partition-Traps festlegen (→ 4.4.5)
- Ziel für Traps und E-Mails über MMB festlegen (→ 4.4.6)
- Sonstige Einstellungen (→ 4.4.7)

Anm.:

- Benutzen Sie das PRIMEQUEST Installation Support Tool, den Installer für Software-Bundle-Packages oder SystemcastWizard Lite, um den PSA zu installieren. Wie Sie den PSA manuell installieren können, ist in Kapitel 4, „Manual PSA Installation“ im Handbuch *PRIMEQUEST 500A/500/400 Series Reference Manual: Tools/Operation Information* (U41757-J-Z816-x-76/C122-E074EN) beschrieben.
  Das PRIMEQUEST Installation Support Tool ist im *PRIMEQUEST Installation Support Tool User's Guide (SUSE)* (C122-E047EN) beschrieben.
  Einzelheiten über den Installer für Software-Bundle-Packages finden Sie im *PRIMEQUEST Bundled-Software Package Installer User's Guide* (C122-E006EN).
  Näheres über SystemcastWizard Lite finden Sie im *PRIMEQUEST SystemcastWizard Lite User's Guide* (C122-E010EN).
- Während der Installation des PSA werden die folgenden für den Betrieb erforderlichen Modifikationen automatisch durchgeführt:
  - Hinzufügen ~~**von**~~ **der** Einstellungen in der **Datei** syslog.conf
  - Hinzufügen ~~**von**~~ **der** Einstellungen in der **Datei** snmpd.conf
  - ~~**Setup**~~ **Hinzufügen der Einstellungen in der Datei** snmptrapd.conf
  - Deaktivieren der automatischen Starteinstellungen von salinfo oder salinfo_decode (*1)

- Deaktivieren der automatischen Starteinstellungen von smartd **(*1)**
- Einfügen der Beschreibung in die Datei services (*2)

*1 Diese automatischen Starteinstellungen sind wegen Konflikten mit einigen PSA-Funktionen deaktiviert.

*2 Hinzugefügter Port:
Es wird nicht überprüft, ob Portnummern doppelt vergeben wurden sind, wenn **~~weitere Daten~~ die Einstellungen** in die Dienstedatei fj-webgate (24450) eingefügt werden. Führen Sie eventuell notwendige Änderungen durch.

[Änderungen (halfett ausgezeichnst) gemäß Manual Errata 2009/02/24]

Anmerkung: Falls die IP-Adresse des MMB oder die des Management-LANs auf seiten der Partition geändert wurde, dürfen Sie nicht vergessen, PSA neu zu starten. Andernfalls kommt es zu einem Anzeigefehler im PSA-Fenster des MMB-Web-UI, und die von PSA registrierten Fehler werden nicht gemeldet.

4.4.1 Einstellungen des Management-LANs überprüfen

In diesem Abschnitt wird beschrieben, wie Sie die Einstellungen des Management-LANs überprüfen können.
Damit der PSA über das Management-LAN mit dem MMB kommunizieren kann, muss die mit dem Management-LAN verbundene NIC (Network Interface Card) der Partition aktiv sein.

(1) Einstellungen für die NIC des Management-LANs überprüfen

Führen Sie das folgende Kommando aus, um den Namen der Schnittstelle zu überprüfen, der dem NIC des Management-LANs zugewiesen ist.

1 Geben Sie das Kommando ifconfig ein, um die vom System erkannten Netzwerkschnittstellen aufzulisten und den betreffenden Schnittstellennamen zu bestätigen.
Kommandosyntax:

```
/sbin/ifconfig –a
```

Beispiel: Die Schnittstellen heißen eth0, eth1 und lo.

```
# /sbin/ifconfig –a
eth0      Link encap:Ethernet  HWaddr 00:D0:B7:53:89:C3
          inet addr:192.168.1.10  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::2d0:b7ff:fe53:89c3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1107704 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2653820 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:390009908 (371.9 MiB)  TX bytes:809006934 (771.5 MiB)

eth1      Link encap:Ethernet  HWaddr 00:0E:0C:21:83:97
          inet addr:192.168.1.12  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20e:cff:fe21:8397/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1538726 errors:0 dropped:0 overruns:0 frame:0
          TX packets:356 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:341051195 (325.2 MiB)  TX bytes:22862 (22.3 KiB)
          Base address:0x5cc0 Memory:fbfe0000-fc000000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:3865 errors:0 dropped:0 overruns:0 frame:0
```

2 Benutzen Sie das ethtool-Kommando, um NICs für das Management-LAN zu finden (zwei NICs für das Management-LAN einer PRIMEQUEST 580A/540A*/580/540/480/440 und ein NIC für das Management-LAN einer PRIMEQUEST 520A*/520/420).
Geben Sie das Kommando für jede der in Schritt 1 aufgeführten Schnittstellen in der unten wiedergegebenen Form ein..
Die NICs des Management-LANs haben Bus-Informationen (SEG:BUS:DEV:FUNC number) wie folgt:

PRIMEQUEST 580A/540A*/580/540/480/440: 0000:01:08.0 und 0000:01:00.0
PRIMEQUEST 520A*/520/420: 0000:01:08.0
Kommandosyntax:

```
/usr/sbin/ethtool –i <interface-name>
```

Beispiel: Die Ergebnisse der drei Kommandoaufrufe für eth0 und eth1 zeigen, dass sie beide den NICs für das Management-LAN zugeordnet sind.

Hinweis: Im folgenden Beispiel wird ein System PRIMEQUEST 580A/540A*/580/540/480/440 verwendet.

*: wird von Fujitsu Technology Solutions nicht unterstützt

```
# /usr/sbin/ethtool -i eth0
     driver: e100
     version: 3.0.27-k2-NAPI
     firmware-version: N/A
     bus-info: 0000:01:00.0      (Entspricht einer NIC für das Management-LAN)

# /usr/sbin/ethtool -i eth1
     driver: e100
     version: 3.0.27-k2-NAPI
     firmware-version: N/A
     bus-info: 0000:01:08.0      (Entspricht einer NIC für das Management-LAN)
```

3 Geben Sie folgendes Kommando für die gefundene NIC für das Management-LAN ein, und notieren Sie die Hardware-Adresse:
Kommandosyntax

```
/sbin/ifconfig  <interface-name>
```

Beispiel: Kommandoaufruf für eth0 und eth1

```
#/sbin/ifconfig  eth0
Link encap:Ethernet HWaddr 00:D0:B7:53:89:C3
inet addr:192.168.1.10 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::2d0:b7ff:fe53:89c3/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1107704 errors:0 dropped:0 overruns:0 frame:0
TX packets:2653820 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:390009908 (371.9 MiB) TX bytes:809006934 (771.5 MiB)

#/sbin/ifconfig  eth1
Link encap:Ethernet HWaddr 00:0E:0C:21:83:97
inet addr:192.168.1.12 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::20e:cff:fe21:8397/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1538726 errors:0 dropped:0 overruns:0 frame:0
TX packets:356 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:341051195 (325.2 MiB) TX bytes:22862 (22.3 KiB)
Base address:0x5cc0 Memory:fbfe0000-fc000000
```

Dieses Beispiel enthält folgende Hardware-Adressen für eth0 und eth1:

- Hardware-Adresse von eth0: 00:D0:B7:53:89:C3
- Hardware-Adresse von eth1: 00:0E:0C:21:83:97

Konfigurieren Sie dann jede NIC für das Management-LAN. Verwenden Sie hierfür einen der folgenden Abschnitte:

- Für eine PRIMEQUEST 580A/540A*/580/540/480/440:
  → (2) Zwei NICs für das Management-LAN duplizieren (PRIMEQUEST 580A/540A*/580/540/480/440)
- Für eine PRIMEQUEST 520A*/520/420:
  → (3) NIC für das Management-LAN einstellen (PRIMEQUEST 520A*/520/420)

(2) Zwei NICs für ein redundantes Management-LAN einrichten (PRIMEQUEST 580A/540A*/580/540/480/440)

- SUSE 9

Um das Management-LAN zu duplizieren, aktivieren Sie die beiden NICs für das Management-LAN in der Partition. Die Duplizierungssoftware (für LAN-Duplizierungen) überträgt den Datenstrom über die entsprechende Übertragungsleitung unter Berücksichtigung des Leitungsstatus und erreicht somit eine Redundanz. Wenn Sie eine Duplizierung festlegen, wird eine virtuelle Schnittstelle generiert, so dass die beiden NICs logisch wie eine NIC funktionieren. Der PSA und andere TCP/IP-Anwendungen verwenden die IP-Adresse der virtuellen Schnittstelle als lokale IP-Adresse des Systems, um mit dem entfernten System zu kommunizieren, ohne eine redundante physikalische Konfiguration berücksichtigen zu müssen.

Die Duplizierung kann über Bonding oder mit PRIMECLUSTER GLS durchgeführt werden. In beiden Fällen wird die Übertragungsleitung zum externen Switch überwacht und im Fehlerfall zur anderen Leitung umgeschaltet.

Wie aus Abbildung 4.3 hervorgeht, wird die Übertragungsleitung von der Partition zum externen Switch dupliziert, indem die Datenwege zum externe Switch, der an die Benutzerports der MMBs angeschlossen ist, mit in die Überwachung eingeschlossen werden.

*: wird von Fujitsu Technology Solutions nicht unterstützt

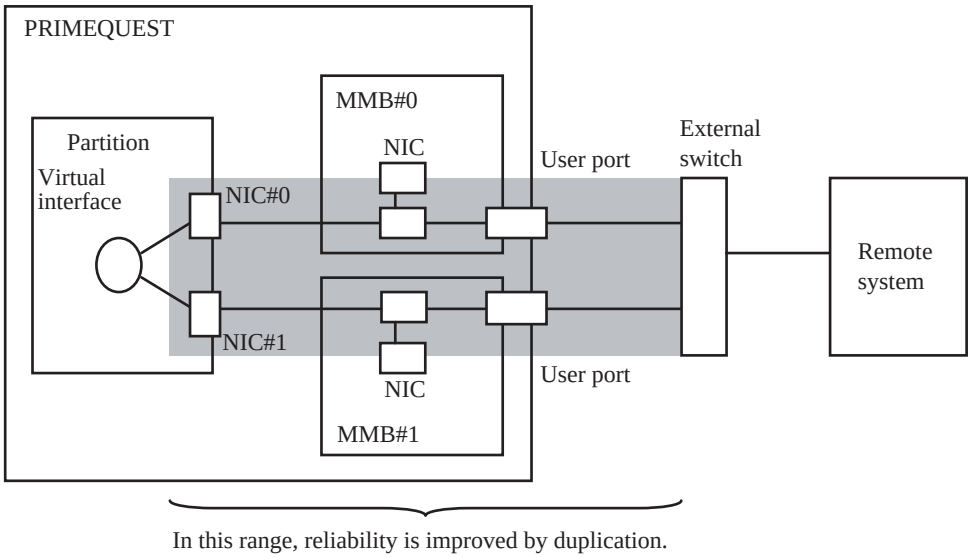


Abbildung 4.3 Konzept eines redundanten PRIMEQUEST-Management-LANs

Zusätzlich kann die Verfügbarkeit erhöht werden, indem der externe Switch und die Datenwege zum entfernten System redundant ausgeführt werden, wie in Abbildung 4.4 gezeigt wird. Die entsprechenden Einstellungen müssen auf dem entfernten System gemacht werden.

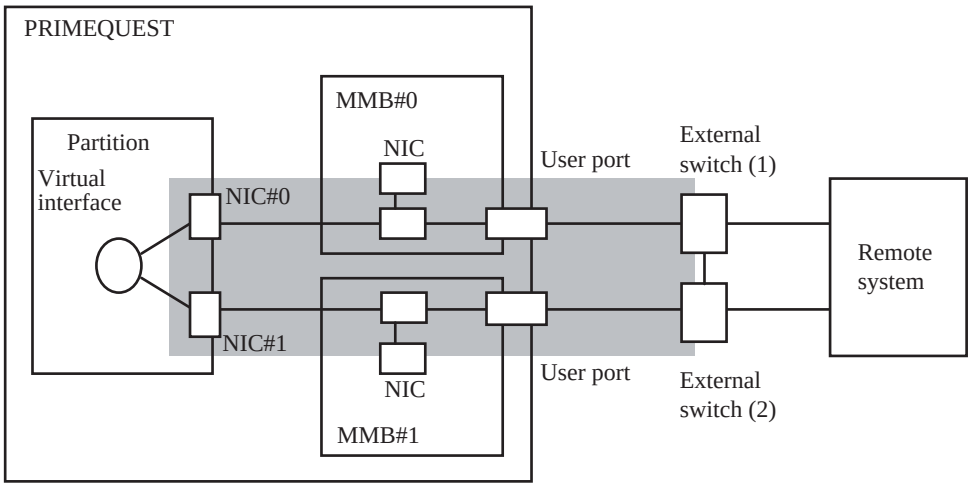


Abbildung 4.4 Konzept eines redundanten PRIMEQUEST-Management-LANs (Konfiguration mit erhöhter Verfügbarkeit)

- Bonding

Hinweis:Ändern Sie die VLAN-Einstellung für den Management-LAN-Hub des MMB in „VLAN Mode“. (Näheres finden Sie unter 2.2.4.5, „Einen Management-LAN-Hub einrichten“.)

1 Bearbeiten Sie die Datei ifcfg für die relevante Schnittstelle in /etc/sysconfig/network/. Legen Sie die Datei an, falls sie nicht existiert. Halten Sie das Netzwerk an, bevor Sie die Datei bearbeiten.

•Bonding Interface: ifcfg-<bonding-interface-name> Beispiel: ifcfg-bond0

Anm.: Falls die relevanten Schnittstellen für das Management-LAN in /etc/sysconfig/network/ liegen, deaktivieren Sie sie durch Löschen.

- Dateiname der Datei ifcfg für das Management-LAN: ifcfg-eth-id-<hardware-address>

● Ausgabe der Datei ifcfg der NIC-Schnittstelle für das Management-LAN

```
# rcnetwork stop
# rm /etc/sysconfig/network/ifcfg-eth-id-<hardware-address>
..
# vi /etc/sysconfig/network/ifcfg- <bonding-interface-name>
```

Ändern oder ergänzen Sie Zeilen, wie im Folgenden gezeigt wird.

Beispiel: Im folgenden Beispiel wird beim Bearbeiten der Datei ifcfg davon ausgegangen, dass das bonding-Interface ifcfg-bond0 ist.

```
ifcfg-bond0:
   BOOTPROTO='static'
   MTU=''
   REMOTE_IPADDR=''
   IPADDR='192.168.16.138'      # Same subnet as the MMB
   NETMASK='255.255.255.0'
   BROADCAST='192.168.16.255'
   STARTMODE='onboot'
   BONDING_MASTER=yes
   BONDING_SLAVE_0='bus-pci-0000:01:08.0'
   # bus-info number for management LAN NIC#0
   BONDING_SLAVE_1='bus-pci-0000:01:00.0'
   # bus-info number for management LAN NIC#1
   BONDING_MODULE_OPTS='arp_interval=1000 arp_ip_target=192.168.16.111,
   192.168.16.112 mode=1'
   # external switch IP address
```

Geben Sie anschließend „start“ für den Netzwerkdienst ein, um das Bonding Interface zu aktivieren.

Kommandosyntax:

```
rcnetwork start
```

PSA muss neu gestartet werden, damit die Einstellungen für den Management-LAN-NIC wirksam werden.

Kommandosyntax:

```
/etc/init.d/y30FJSVpsa stop
/etc/init.d/y30FJSVpsa start
```

- PRIMECLUSTER GLS

  Eine Beschreibung der für die Duplizierung des Management-LANs mit PRIMECLUSTER GLS erforderlichen Einstellungen finden Sie im Handbuch für PRIMECLUSTER GLS. Um PRIMECLUSTER GLS anzuwenden, müssen die externen Switches am Benutzerport des MMB in Abbildung 4.3 und Abbildung 4.4 als überwachte Hubs eingerichtet werden.

  Hinweis: Wenn für das Management-LAN bereits ein Netzwerk konfiguriert wurde, benutzen Sie für PRIMECLUSTER GLS die IP-Adresse aus der ifcfg-Datei und folgen Sie bei der Konfiguration der Duplikation den Anweisungen des PRIMECLUSTER GLS Handbuchs.

  Wenn Sie die Einstellungen für die Duplikation über GLS gemacht haben, starten Sie den Netzwerkdienst und den PSA neu.

  Kommandosyntax:

```
/sbin/service y30FJSVpsa stop
/sbin/service y30FJSVpsa start
```

- SUSE 10

  1 Fügen Sie am Ende der Datei /etc/modprobe.conf.local untenstehende Zeile ein. Benennen Sie die Bonding-Schnittstelle (bondN, wobei N eine Zahl in aufsteigender Folge ist, wie 0, 1, 2...).

```
# vi /etc/modprobe.conf.local

Add the following line to the end of the file:
alias <Bonding interface-name> bonding
options <Bonding interface-name> mode=1 arp_interval=1000
arp_ip_target=<external-switch-IP-address>// (*1)
```

*1 Geben Sie für die in Abbildung 4.5 gezeigte Konfiguration eine IP-Adresse an. Für die Konfiguration in Abbildung 4.6 geben Sie zwei IP-Adressen an.

```
options <Bonding interface-name> arp_ip_target=<external-switch-IP-address(1)> , <external-switch-IP-address(2)>
```

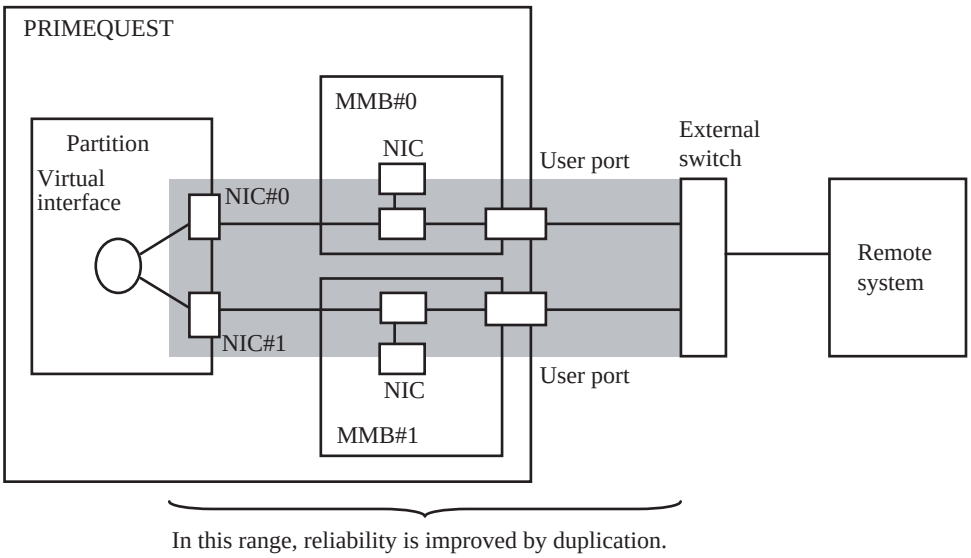


Abbildung 4.5 Duplizierung des Management-LAN bei PRIMEQUEST

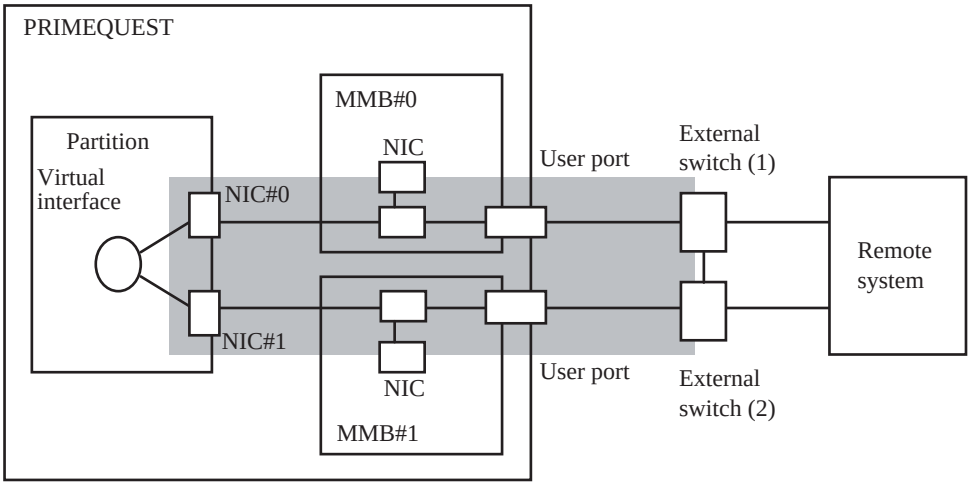


Abbildung 4.6 Duplizierung des Management-LAN bei PRIMEQUEST (Konfiguration mit verbesserter Zuverlässigkeit)

2 Öffnen Sie die Datei ifcfg für die betreffende Schnittstelle in /etc/sysconfig/network/. Erstellen Sie die Datei, falls sie nicht existiert. Um die Datei auszugeben, halten Sie das Netzwerk erst an.

- Bonding Schnittstellen-Bezeichnung: ifcfg-<Bonding interface-name>
  Beispiel: ifcfg-bond0

Hinweis: Befindet sich die betreffende Schnittstelle für das Management-LAN in /etc/sysconfig/network/, deaktivieren Sie sie durch Löschen.

- Name der Datei ifcfg der Schnittstelle für das Management-LAN: ifcfg-eth-id-<hardware-address>

● Ausgabe der Datei ifcfg der NIC-Schnittstelle interface für das Management-LAN

```
# rcnetwork stop
# rm /etc/sysconfig/network/ifcfg-eth-id-<hardware-address>
..
# vi /etc/sysconfig/network/ifcfg-<Bonding interface-name>
```

Ändern oder ergänzen Sie Zeilen, wie im Folgenden gezeigt wird.

Beispiel: Im folgenden Beispiel wird beim Bearbeiten der Datei ifcfg davon ausgegangen, dass das bonding-Interface ifcfg-bond0 ist.

```
ifcfg-bond0:
BOOTPROTO='static'
MTU=''
REMOTE_IPADDR=''
IPADDR='192.168.16.138' # Same subnet as the MMB
NETMASK='255.255.255.0'
BROADCAST='192.168.16.255'
STARTMODE='onboot'
BONDING_MASTER=yes
BONDING_SLAVE_0='bus-pci-0000:01:08.0'
# bus-info number of the NIC for management LAN#0
BONDING_SLAVE_1='bus-pci-0000:01:00.0'
# bus-info number of the NIC for management LAN#1
```

Die Bonding-Schnittstelle wird beim Neustart des Netzwerk-Dienstes aktiviert.

Kommandosyntax

```
/sbin/service network restart
```

PSA muss neu gestartet werden, damit die Einstellungen für den Management-LAN-NIC wirksam werden.

Kommandosyntax

```
/etc/init.d/y30FJSVpsa stop
/etc/init.d/y30FJSVpsa start
```

(3) NIC für das Management-LAN einstellen (PRIMEQUEST 520A*/520/420)

Der Management-LAN-NIC muss in der Partition aktiviert werden, damit er über das Management-LAN mit den MMBs kommunizieren kann. Konfigurieren Sie den NIC wie im folgenden beschrieben. Verwenden Sie hierzu YaST.

1 Führen Sie das folgende Kommando aus, und speichern Sie den Namen des Controllers des Management-LAN-NIC:
Kommandosyntax

```
/sbin/lspci -s 0000:01:08.0
```

Beispiel: In diesem Beispiel lautet der Name des Controllers „Intel Corporation 82562ET/EZ/GT/GZ - PRO/100 VE (LOM) Ethernet Controller“.

```
# /sbin/lspci -s 0000:01:08.0
01:08.0 Ethernet controller: Intel Corporation 82562ET/EZ/
GT/GZ - PRO/100 VE (LOM) Ethernet Controller (rev 04)
```

2 Geben sie folgendes Kommando ein, um YaST zu starten.
Kommandosyntax:

```
# yast
```

3 Wählen Sie im Menü [Network Devices] - [Network Card], und wechseln Sie in das Fenster mit der Auswahl der Netzwerkkarten.

4 Aus den im Fenster [Network Card Configuration] gezeigten Karten wählen Sie die Karte (Management-LAN-NIC) mit dem Namen, den Sie in Schritt 1 gespeichert haben.

Hinweis:Möglicherweise wird der Name, den Sie in Schritt 1 gespeichert haben, entsprechend der YaST-Spezifikation nicht komplett angezeigt. Wie in Abbildung 4.7 wird evtl. „Fujitsu“ dem Namen des Controllers vorangestellt und nur der letzte Teil seines Namens ausgegeben. In diesem Fall wählen Sie den Namen aus, bei dem die ausgegebene Buchstabenfolge mit Ausnahme von „Fujitsu“ dem letzten Teil des in Schritt 1 gespeicherten Namens entspricht.

*: wird von Fujitsu Technology Solutions nicht unterstützt

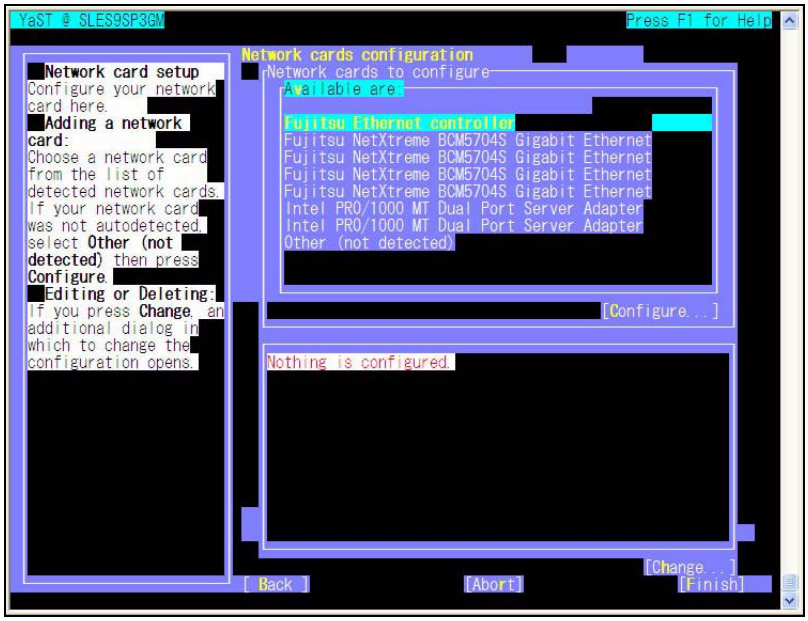

YaST @ SLES9SP3GM
Press F1 for Help
Network card setup
Configure your network card here.
Adding a network card:
Choose a network card from the list of detected network cards. If your network card was not autodetected, select Other (not detected) then press Configure.
Editing or Deleting:
If you press Change, an additional dialog in which to change the configuration opens.
Network cards configuration
Network cards to configure
Available are:
Fujitsu Ethernet controller
Fujitsu NetXtreme BCM5704S Gigabit Ethernet
Fujitsu NetXtreme BCM5704S Gigabit Ethernet
Fujitsu NetXtreme BCM5704S Gigabit Ethernet
Fujitsu NetXtreme BCM5704S Gigabit Ethernet
Intel PRO/1000 MT Dual Port Server Adapter
Intel PRO/1000 MT Dual Port Server Adapter
Other (not detected)
[Configure...]
Nothing is configured.
[Change...]
[Back]
[Abort]
[Finish]

Abbildung 4.7 YaST-Fenster

* Dieses Beispiel zeigt ein SUSE9-Fenster. Der Inhalt kann abhängig vom Betriebssystem abweichen.

* In diesem Fall entspricht der zweite Menüpunkt (Fujitsu Ethernet-Controller) dem letzten Teil des in Schritt 1 gespeicherten Namens.

5 Wechseln Sie in das Fenster [Network Address Setup], und installieren Sie die Netzwerkkarte.

Bestätigen Sie, dass der Wert von [Configuration Name] die Hardware-Adresse enthält, die unter (1), „Einstellungen für die NIC des Management-LANs überprüfen“ eingestellt wurde. Wählen Sie [Static address setup], und geben Sie IP-Adresse und Subnetz-Maske an.

Hinweis: Die angegebene IP-Adresse und die IP-Adresse des MMB müssen die gleiche Subnetz-Maske haben.

6 Verlassen Sie YaST.

4.4.2 Kontrollfunktionen für syslog

Sollten Sie SUSE™ Linux Enterprise Server 10 verwenden, müssen sie folgende Zusatzeinstellungen vornehmen.

Hinweis: Versäumen Sie es, die folgenden Einstellungen vor der Installation von PSA vorzunehmen, könnte folgende Meldung erscheinen und PSA kann evtl. die Treiber-Meldungen nicht überwachen.
syslogd: /var/opt/FJSVpsa/path/syslogd.fifo: Operation not permitted

Anm.: Benutzen Sie die Tasten [↑] und [↓], um den Cursor auf dem YaST-Bildschirm auf und ab zu bewegen.

1 Geben Sie folgendes Kommando ein, um den aktiven Syslog-Dämon zu überprüfen.

```
# grep SYSLOG_DAEMON /etc/sysconfig/syslog
```

If SYSLOG_DAEMON = Wenn „syslog-ng“ für SYSLOG_DAEMON ausgegeben wird, läuft /sbin/syslog-ng als Syslog-Dämon.

If SYSLOG_DAEMON = Wenn „syslog“ für SYSLOG_DAEMON ausgegeben wird, läuft /sbin/syslogd als Syslog-Dämon.

Speichern sie den Namen des laufenden Syslog-Dämons.

2 Ändern Sie die Einstellungen für AppArmor mit folgender Prozedur:

1) Starten Sie YaST.

```
# yast
```

Abbildung 4.8 Yast Startbildschirm

2) Aus dem Menü auf der linken Seite von Abbildung 4.9, wählen Sie „Novell AppArmor“ und drücken die Taste [Tab].
Wählen Sie als nächstes aus dem Menü auf der rechten Seite „Edit Profile“ und drücken Sie [Enter].

Abbildung 4.9 Bildschirm Novell AppArmor-select

3 Bewegen Sie sich mit Hilfe von [Tab] auf „Profile Name“, um „Profile Name“ auf den aktiven Syslog-Dämon hin zu überprüfen. Der aktive Syslog-Dämon ist der, der in Schritt 1 bestätigt wurde.
Wenn Sie den aktiven Syslog-Dämon unter „Profile Name“ nicht finden, müssen die folgenden Einstellungen gemacht werden. Wählen Sie in diesem Fall „Abort“ aus der unteren Menüzeile, und drücken Sie [Enter], um dieses Fenster zu verlassen. Dann wählen Sie „Quit“ aus der unteren Menüzeile und drücken [Enter], um YaST zu verlassen.
Finden Sie den aktiven Syslog-Dämon unter „Profile Name“, wählen Sie den Namen des Syslog-Dämons aus. Dann wählen Sie mit der [Tab]-Taste „Next“ aus der unteren Menüzeile und drücken [Enter].

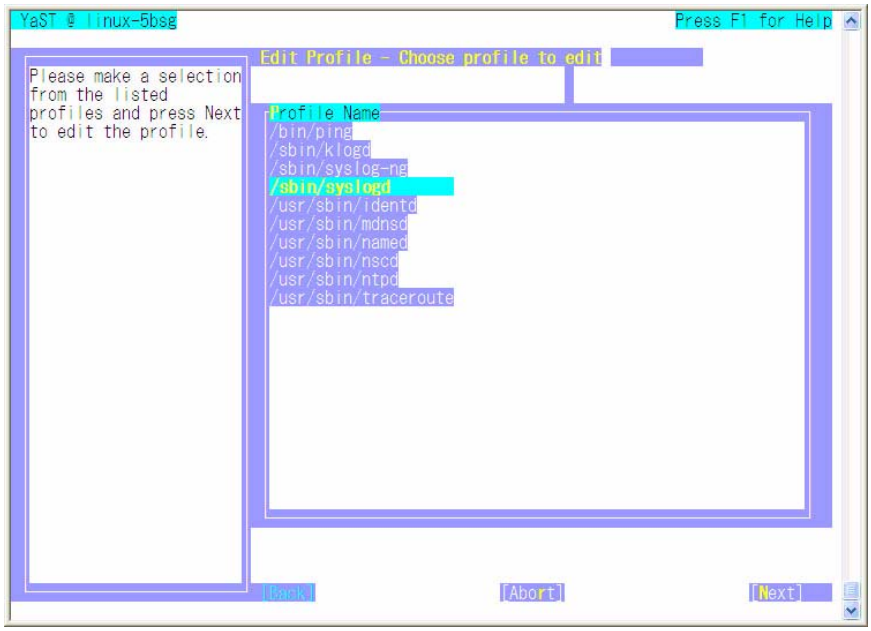
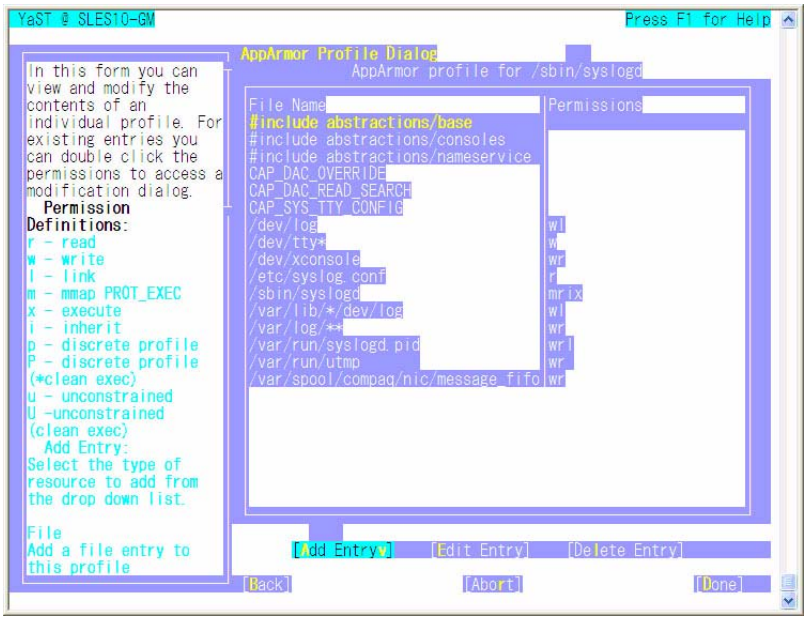


Abbildung 4.10 Bildschirm AppArmor Profile select

4 Wählen Sie mit der [Tab]-Taste „Add Entry“ aus der unteren Menüzeile aus, und drücken Sie [Enter].



Wählen Sie „File“ in der Ausgabeliste, und drücken Sie [Enter].

Abbildung 4.11 Bildschirm Entry addition and selection

5 Geben Sie „/var/opt/FJSVpsa/path/syslog_fifo“ im Feld „Enter or modify Filename“ ein, und drücken Sie [Tab].
Als nächstes markieren Sie im Feld „Permissions“ mithilfe der [Space]-Taste die „Read“- und „Write“-Check-Boxen.
Wählen Sie mit der [Tab]-Taste OK, und drücken Sie [Enter].

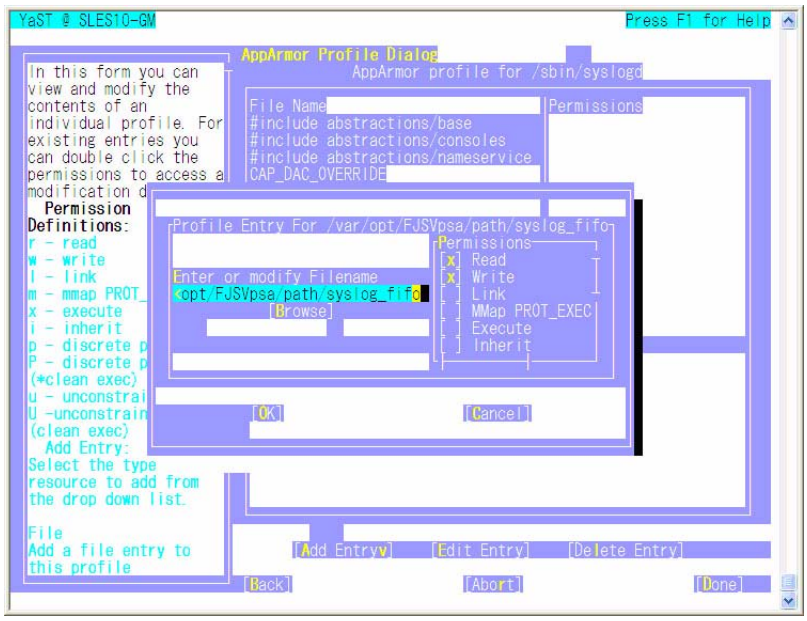


Abbildung 4.12 Bildschirm Adding the Profiles Entry

6 Überprüfen Sie, ob die in Schritt 5 gemachten Änderungen umgesetzt wurden.

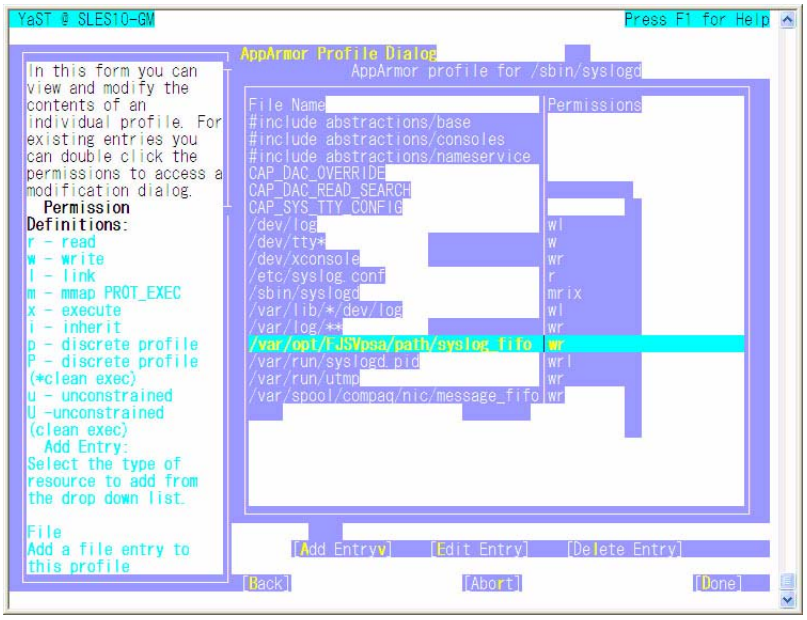


Abbildung 4.13 Bildschirm Entry list

7 Wählen Sie mit der [Tab]-Taste „Done“ aus der unteren Menüzeile. Daraufhin erscheint der Bildschirm [Save changes to the Profile].
Im Bildschirm [Save changes to the Profile] wählen Sie [Yes], und drücken Sie [Enter].

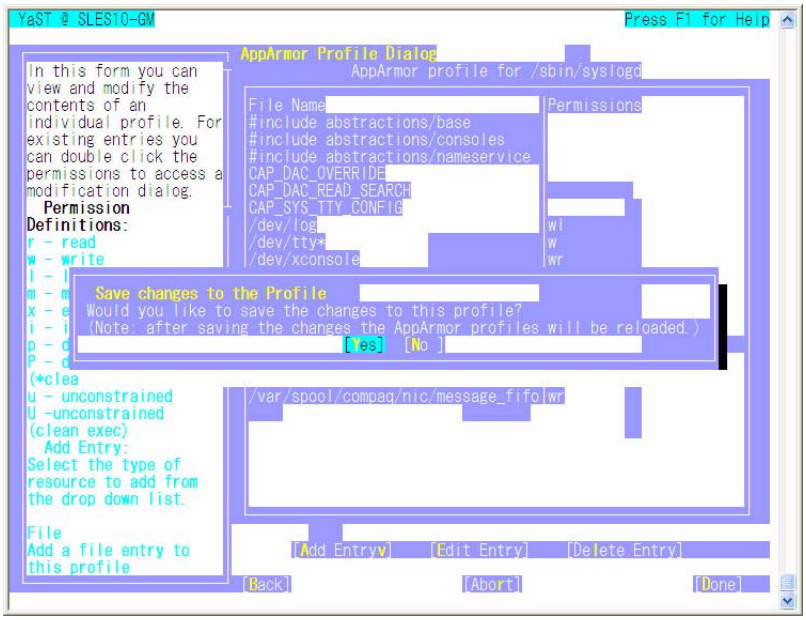


Abbildung 4.14 Bildschirm Saving the profiles

8 Wählen Sie mit [Tab] „Quit“ aus der unteren Menüzeile, und drücken Sie [Enter], um YaST zu verlassen.

9 Starten Sie AppArmor neu.

```
# /etc/init.d/boot.apparmor restart
Reloading AppArmor profiles                                done
```

10 Starten Sie die Syslog-Dienste neu.

```
# /etc/init.d/syslog restart
Shutting down syslog services                              done
Starting syslog services                                   done
```

4.4.3 SELinux-Funktion

Standardmäßig ist die SELinux-Funktion auf den PRIMEQUEST-Systemen deaktiviert. Verwenden Sie die SELinux-Funktion nicht.

4.4.4 Firewall überprüfen (Ports freigeben)

Wenn der Port nicht freigegeben wurden, als die Firewall-Einstellungen gemacht wurden, geben Sie nun die für den PSA-Betrieb erforderlichen Ports des Management-LANs frei. Geben Sie insbesondere die folgenden Ports frei:

- snmp-Port : udp / snmp oder 161
- snmptrap-Port : udp / snmptrap oder 162 (*1) (zur physikalischen IP-Adresse des MMBs (beide Systeme))
- web-mmb Kommunikationsport: tcp / fj-webgate oder 24450 (*2) (zur virtuellen IP-Adresse des MMBs)
- rmcp+-Port : udp/7000 bis 7100 (*1) (zur physikalischen IP-Adresse des MMBs (beide Systeme))
- snmp-Port des lokalen Rechners: udp/1025-65535
- psa-mmb Kommunikationsport: Port 5000 für tcp/MMB (*3) (zur virtuellen IP-Adresse des MMBs) icmp/icmp-Typ0, icmp-Typ8 (zur virtuellen IP-Adresse des MMBs)

*1 Geben Sie den Port nur frei, wenn eine PCL-Verbindung verwendet wird. Überprüfen Sie die Firewall-Einstellungen mit dem Kommando iptables.

*2 web-mmb Kommunikationsport

*3 Dies ist der Kommunikationsport 5000 für MMB.
Da die Partition in dieser Kommunikation als Client fungiert, ist die Portnummer auf Partition-Seite undefiniert. (Eine beliebige Nummer von tcp/1025 bis 65535 wird für einen Port ausgewählt.)
Wie das folgende Beispiel zeigt, ist darüber hinaus keine Einstellung für Portnummer 5000 verlangt, wenn der Verbindungsaufbau von der Partition aus möglich ist oder wenn die Kommunikation für die Verbindung mit der eingerichteten Partition möglich ist.

(Beispiel) iptables -A OUTPUT -m state --state NEW,ESTABLISH -j ACCEPT
iptables -A INPUT -m state --state ESTABLISH -j ACCEPT

Kommandosyntax:

```
/sbin/iptables –L
```

Geben Sie ein Port mithilfe des Kommandos iptables oder eines anderen Kommandos frei. Näheres finden Sie in den Manual Pages des Betriebssystems.

Kommandosyntax:

```
/usr/bin/man iptables
```

4.4.5 Ziel für Partition-Traps festlegen

Hinweise:

- Machen Sie diese Einstellung nur, wenn sie erforderlich ist.
- Die Einstellung ist für die Verbindung zu einer Betriebsverwaltungs-software erforderlich.

Das Ziel der SNMP-Traps muss auf der Partition eingestellt werden. Fügen Sie das Ziel in die Datei snmpd.conf ein.

- Datei snmpd.conf modifizieren

```
# vi /etc/snmpd.conf

Add the following lines for the SNMP version to be used.  The lines can be provided in any order.
trapsink HOST [COMMUNITY [PORT]]   # SNMPv1 trap setting
trap2sink HOST [COMMUNITY [PORT]] # SNMPv2 trap setting
trapsess SNMPCMD_ARGS HOST[:PORT] # SNMPv3 trap setting
```

In unserem Beispiel sind folgende Einstellungen erforderlich:

- SNMPv1/SNMPv2-Traps einstellen

```
trapsink HOST [COMMUNITY [PORT]]   # SNMPv1 trap setting
trap2sink HOST [COMMUNITY [PORT]] # SNMPv2 trap setting
```

Geben Sie den Host an, an den die Traps gesendet werden sollen.

- Bei dieser Einstellung wird eine Kaltstart-Trap übertragen, wenn snmpd gestartet wird. Wenn die Übertragung von SMNP-Traps festgelegt wurde, dann wird auch im Falle einer fehlgeschlagenen Authentifizierung eine Trap übertragen.
- Indem Sie mehrere Zeilenpaare für trapsink und trap2sink in die Datei einfügen, können Sie für die Traps mehrere Ziele festlegen.
- Wenn COMMUNITY nicht festgelegt wurde, wird die Zeichenkette verwendet, die zuvor von der trapcommunity-Anweisung festgelegt wurde.
  Mit dem Kommando trapcommunity wird die Standardzeichenkette für die Übertragung von Traps festgelegt. Geben Sie bei Verwendung dieses Kommandos die String vor dem Zeilenpaar trapsink-trap2sink ein.

```
trapcommunity STRING                    #COMMUNITY name setting
```

- Wenn kein spezifischer Port angegeben wird, wird der Standardport für SNMP-Traps (162) benutzt.

Beispiel: Wenn Sie Traps mit dem Community-Name „public“ an den Port 162 des Managementsystem mit der IP-Adresse 192.168.1.10 senden wollen:

```
trapsink  192.168.1.10  public  162          ##SNMPv1 trap setting
trap2sink  192.168.1.10  public  162         ##SNMPv2 trap setting
```

- Trap-Einstellungen für SNMPv3

```
trapsess SNMPCMD_ARGS HOST[:PORT]    #SNMPv3 trap setting
```

Geben Sie den Host an, an den die Traps gesendet werden sollen. Wenn kein spezifischer Port angegeben wird, wird der Standardport für SNMP-Traps (162) benutzt.

Die folgenden Optionen stehen für SNMPCMD_ARGS zur Verfügung:

-v version : SNMP-Version. Geben Sie für SNMPv3 eine 3 an.

-e engineID: Die oldEngineID aus der Datei /var/net-snmp/snmpd.conf des Trap-Senders.

-u secName: Das SNMPv3-Benutzerkonto. Dieselbe Einstellung wie beim Managementsystem ist erforderlich.

-l secLevel : Je nach Sicherheitsstufe der SNMPv3-Meldungen, eine der folgenden Optionen:

Tabelle 4.4 Sicherheitsstufen

Einstellung	Authentifizierung	Verschlüsselung
noAuthNoPriv	Nein	Nein
authNoPriv	Ja	Nein
authPriv	Ja	Ja

-a authProtocol: Legt MD5 oder SHA als verwendetes Protokoll für die Authentifizierung von SNMPv3-Meldungen fest. Bei SHA muss ein Paket mit dem installierten openssl erstellt werden. Diese Option ist gültig, wenn in der mit der Option -l festgelegten Sicherheitsstufe eine Authentifizierung enthalten ist. Wenn keine Authentifizierung enthalten ist, kann diese Option entfallen.

-A authPassword: Legt das Kennwort für die Authentifizierung fest (mindestens 8 Zeichen). Es muss sich um dasselbe Kennwort wie beim Managementsystem handeln. Diese Option gilt, wenn in der mit der Option -l festgelegten Sicherheitsstufe eine Authentifizierung enthalten ist. Wenn keine Authentifizierung enthalten ist, kann diese Option entfallen.

-x privProtocol: Legt das Verschlüsselungsverfahren für SNMPv3-Meldungen fest. Aktuell wird nur DES unterstützt. Diese Option gilt, wenn in der mit der Option -l festgelegten Sicherheitsstufe eine Verschlüsselung vorgesehen ist. Wenn keine Verschlüsselung vorgesehen ist, kann diese Option entfallen.

-X privPassword: Legt ein verschlüsseltes Kennwort fest (mindestens 8 Zeichen). Es muss sich um dasselbe Kennwort wie beim Managementsystem handeln. Diese Option gilt, wenn in der mit der Option -l festgelegten Sicherheitsstufe eine Verschlüsselung vorgesehen ist. Wenn keine Verschlüsselung vorgesehen ist, kann diese Option entfallen.

Beispiel: SNMPv3-Traps sollen mit dem Benutzerkonto „PRIMEQUEST“ mit Authentifizierung und Verschlüsselung an den Port 162 des Managementsystems mit der IP-Adresse 192.168.1.10 gesendet werden:

```
#trapsess 3 -e 0x800007e58026577a9f421950a4 -u PRIMEQUEST -l authPriv
-a MD5 -A 00000000
-x DES -X 11111111 192.168.1.10:162      ##SNMPv3 trap setting
```

Wenn das Ziel für die Übertragung der Traps festgelegt ist, starten Sie snmpd mit dem folgenden Kommando neu:

```
#/etc/init.d/snmpd restart
```

Aktivieren Sie PSA, nachdem snmpd reaktiviert wurde.

```
#/etc/init.d/y30FJSVpsa y30FJSVpsa stop
#/etc/init.d/y30FJSVpsa y30FJSVpsa start
```

Einstellungen des Trap-Ziels überprüfen

Verwenden Sie die standardmäßige net-snmp-Trap, mit der snmpd neu gestartet werden würde, um die Einstellungen für das Trap-Ziel zu überprüfen. Überprüfen Sie, ob die Trap ordnungsgemäß am Ziel empfangen wird.

Anm.: Am Trap-Ziel muss eine entsprechende Anwendung aktiviert sein, damit die Traps empfangen werden können.

Starten Sie snmpd neu, indem Sie auf dem Ausgangssystem das folgende Kommando ausführen:

```
# /etc/init.d/snmpd restart
```

Die Trap-Anwendung auf dem Zielrechner erhält die Standardmeldung „ColdStart“.

Handelt es sich bei dem Zielrechner beispielsweise um einen Linux-Rechner, wird die folgende Meldung in die Datei syslog geschrieben, wenn snmptrapd eine Trap erhält. Das zeigt, dass das Zielgerät Traps ordnungsgemäß empfängt.

Aug 17 12:00:53 pq-server snmptrapd[2600]: 2005-08-17 12:00:53 pq-server.fujitsu.com [192.168.1.10](via 192.168.1.10) TRAP, SNMP v1, community public NET-SNMP-MIB::netSnmpAgentOIDs.10 Cold Start Trap (0) Uptime: 0:00:00.17

Anm.: Falls das Betriebssystem SUSE™ Linux Enterprise Server 9 Service Pack 2 ist und direkte Meldung zum SNMP-Manager eingestellt ist, wird „0.0.0.0“ in den Trap-Daten als Agent Address im SNMP-Layer gemeldet. Deshalb kann der SNMP-Manager die IP-Adresse der Trap-Quelle der Agent Address nicht entnehmen. Einem PSA Expansion Trap kann jedoch die Herkunft entnommen werden, die einen Host-Namen beinhaltet.
IP-Adressen werden im IP Layer gemeldet. Um die IP-Adresse als Identifikation für die Trap-Quelle verwenden zu können, muss „%b“ als snmptrapd-Parameter angegeben werden, ebenso beim Empfang durch den SNMP-Manger, der snmptrapd verwendet. Auf diese Weise enthalten die Trap-Daten die IP-Adresse, die die Trap-Quelle identifiziert. Einzelheiten finden Sie in der Manual Page zu snmptrapd (Aufruf: `man snmptrap`.

4.4.6 Ziel für Traps und E-Mails über MMB festlegen

Hinweise:

- Machen Sie diese Einstellung nur, wenn sie erforderlich ist.
- Die Einstellung ist für die Verbindung zu einer Betriebsverwaltungssoftware erforderlich (z. B. Systemwalker).

Das Ziel für Traps und E-Mails kann mit der MMB Web-UI eingestellt werden.

Näheres über das MMB Trap-Ziel finden Sie in Abschnitt 5.1.2, „SNMP einrichten“. Näheres über das E-Mail-Ziel finden Sie in Abschnitt 2.2.3.5, „SMTP-Einstellungen“.

4.4.7 Sonstige Einstellungen

Anm.: Machen Sie diese Einstellungen nur, wenn sie erforderlich sind.

- Diese Einstellung ist erforderlich, wenn ein repliziertes Laufwerk eingesetzt wird. Sie können eine neue Partition erstellen, indem Sie ein Laufwerk einer Partition desselben Schranks kopieren. In diesem Fall muss die EngingID von SNMPv3 geändert werden, die vom PSA für die interne Kommunikation verwendet wird. Die EngineID kann mit root-Berechtigung wie folgt geändert werden:

1 Überprüfen Sie mit dem Kommando ps, ob der PSA aktiv ist.

Kommandosyntax:

```
ps ax | grep psa
```

Beispiel: Wenn unter /opt/FJSVpsa/bin/ die folgenden Prozesse aufgeführt werden, ist der PSA aktiv.

```
# ps ax | grep psa
 4562 ?        S      0:00 /opt/FJSVpsa/bin/pm -o 70 /etc/opt/FJSVpsa/
global/pmpsa.conf
 4563 ?        S      0:18 /opt/FJSVpsa/bin/loggetd -p /
 4564 ?        S      0:06 /opt/FJSVpsa/bin/sisp -p /
 4565 ?        S      0:00 /opt/FJSVpsa/bin/mmbm -p /
 4566 ?        S      0:01 /opt/FJSVpsa/bin/mmbs -p /
 4567 ?        S      0:02 /opt/FJSVpsa/bin/fs -p /
 4568 ?        S      0:00 /opt/FJSVpsa/bin/ciipmi -p /
 4569 ?        S      7:40 /opt/FJSVpsa/bin/cilog -p /
 4570 ?        S      8:47 /opt/FJSVpsa/bin/cios -p /
 4578 ?        S      0:00 /opt/FJSVpsa/bin/cisalchild 1 /
 4819 ?        Sl     0:00 /opt/FJSVpsa/bin/webgate -p /
 21670 pts/5   S+     0:00 grep psa
```

2 Wenn der PSA aktiv ist, deaktivieren Sie ihm mit dem Kommando stop.

Kommandosyntax:

```
/etc/init.d/y30FJSVpsa stop
```

3 Führen Sie das Kommando ps aus, um zu überprüfen, ob snmpd aktiv ist.

Kommandosyntax:

```
ps ax | grep snmpd
```

Beispiel: snmpd ist aktiv, wenn /usr/sbin/snmpd angezeigt wird.

```
# ps ax | grep snmpd
32611 ?        S      0:04 /usr/sbin/snmpd -Lsd -Lf /dev/null -p /var/run/
snmpd -a
```

4 Wenn snmpd aktiv ist, führen Sie das Kommando service aus, um snmpd zu deaktivieren.

Kommandosyntax:

```
/etc/init.d/snmpd stop
```

5 Ändern Sie den Wert für oldEngineID in der Datei /var/net-snmp/snmpd.conf.

Anm.: Sie können einen beliebigen Wert aus max. 34 Hexadezimalzahlen wählen. Der Wert muss innerhalb der Partitionen eines Schrankes einmalig sein.

Beispiel: Der Wert für oldEngineID wird in 0x19760523 geändert.

```
#vi /var/lib/net-snmp/snmpd.conf
oldEngineID 0x19760523
```

6 Führen Sie folgendes Kommando aus, um snmpd zu aktivieren.

Kommandosyntax:

```
/etc/init.d/snmpd start
```

7 Wechseln Sie in das Verzeichnis /opt/FJSVpsa/sh/, um das Kennwort für snmpv3 für die interne Kommunikation des PSA neu zu generieren.

Kommandosyntax:

```
cd /opt/FJSVpsa/sh/
```

8 Führen Sie in dem genannten Verzeichnis das Kommando snmpsetup.sh aus. Damit wird das snmpv3-Kennwort automatisch generiert, das für die interne Kommunikation des PSA verwendet wird.

Kommandosyntax:

```
./snmpsetup.sh install
```

9 Starten Sie den PSA.

Kommandosyntax:

```
/etc/init.d/y30FJSVpsa start
```

4.4.8 PSA-Update installieren

Führen Sie die folgenden Kommandos in der angegebenen Reihenfolge aus, deaktivieren Sie den PSA und installieren Sie das PSA-Paket neu.

Hinweis: Wenn PEXU gemountet ist, benutzen Sie PSA ab Version1.10.

Kommandosyntax:

Update von PSA-1.2.X-X oder höher

```
/sbin/service y30FJSVpsa stop
/bin/rpm -Uvh FJSVpsa-X.X.X-X.ia64.rpm
/sbin/service y30FJSVpsa start
```

Update von PSA-1.1.X-X

```
/sbin/service y30FJSVpsa stop
/bin/rpm -Uvh FJSVpsa-X.X.X-X.ia64.rpm
/sbin/service y10FJSVpsa start
/sbin/service y30FJSVpsa start
```

* X.X.X-X ist die PSA-Versionsnummer.

4.4.9 PSA deinstallieren

Führen Sie die folgenden Kommandos in der angegebenen Reihenfolge aus, deaktivieren Sie den PSA und deinstallieren Sie das PSA-Paket.

Kommandosyntax:

```
/etc/init.d/y30FJSVpsa stop
/bin/rpm -e FJSVpsa
```

[Beginn des Zusatzes gemäß Manual Errata 2009/02/24]

Bei der Deinstalltion automatisch vorgenommene Einstellungen

Die folgenden Modifikationen werden bei der PSA-Deinstallation automatisch wirksam:

- Löschen der Einstellungen in der Datei syslog.conf
- Löschen der Einstellungen in der Datei snmpd.conf
- Löschen der Einstellungen in der Datei snmptrapd.conf
- Aktivierung der automatischen Starteinstellungen von salinfo oder salinfo_decode
- Aktivierung der automatischen Starteinstellungen von smartd
- Löschen der Einstellungen in der Datei services
- Ändern der Boot-Option snmptrapd

[Ende des Zusatzes gemäß Manual Errata 2009/02/24]

4.5 PSA installieren (Windows Server 2003) (PRIMEQUEST 580A/540A*/580/540/480/440)

In diesem Abschnitt wird die Installation des PSA beschrieben.

Obligatorische Aufgaben:

- Einstellungen für das Management-LAN überprüfen (→ 4.5.1)

Optionale Aufgaben:

- Ziel für Partition-Traps einstellen (→ 4.5.2)
- Ziel für Traps und E-Mails über MMB festlegen (→ 4.5.3)
- Windows-Firewall einstellen (→ 4.5.4)
- Watchdog-Überwachung nach Auftreten eines Stopp-Fehlers (eines schwerwiegenden Systemfehlers) (→ 4.5.5)

Hinweise:

- Benutzen Sie den PRIMEQUEST Software Installer oder Systemcast-Wizard Lite, um den PSA zu installieren. Wie Sie den PSA manuell installieren können, ist in Kapitel 4, „Manual PSA Installation“ im *PRIMEQUEST 500A/500/400 Series Reference Manual: Tools/Operation Information* (U41757-J-Z816-x-76/C122-E074EN) beschrieben.
  Näheres über eine Installation mit dem PRIMEQUEST Software Installer finden Sie in Abschnitt 3.3.6.1, „Installation mit PRIMEQUEST Software Installer“.
  Die Installation mit SystemcastWizard Lite ist im *PRIMEQUEST SystemcastWizard Lite User's Guide* (C122-E010EN) beschrieben.
- Bei der Installation des PSA werden die folgenden für den Betrieb erforderlichen Einstellungen automatisch durchgeführt:

1 Einstellung der Dienste
- PRIMEQUEST Server Agent
- PRIMEQUEST PEM Command Service
- PRIMEQUEST PSA Environment Control Service

2 Einstellen der Umgebungsvariablen
- Variable PATH
  Der von PSA zu verwendende Wert wird der bestehenden PATH-Variable hinzugefügt.

*: wird von Fujitsu Technology Solutions nicht unterstützt

- Variable FJSVpsa_INSTALLPATH
  Diese Variable wird neu hinzugefügt.

3 Port-Einstellungen
  Es wird damit sichergestellt, dass PSA den Port TCP:24450 verwendet.

4 SNMP-Sicherheitseinstellungen
  Machen Sie die erforderlichen Sicherheitseinstellungen für den SNMP-Dienst, da der PSA vom MMB SNMP-Pakete empfangen muss.
  Die weitere Vorgehensweise hängt von dem Parameter ab, der während der Installation des PSA auf dem Registerblatt [Security] des Fensters [Properties] für [SNMP Service] ausgewählt wird.

- Wenn [Accept SNMP packets from any host] ausgewählt wird:
  SNMP-Sicherheitseinstellungen sind nicht erforderlich.
- Wenn [Accept SNMP packets from these hosts] ausgewählt wird:
  Richten Sie mit Ihren Einstellungen eine sichere SNMP-Übertragung ein, wenn die IP-Adresse des MMB und der Parameter für den lokalen Host nicht angegeben sind.

  Hinweis: Wenn Sie die Einstellung nach der Installation des PSA von [Accept SNMP packets from any host] in [Accept SNMP packets from these hosts] ändern wollen, oder wenn Sie die IP-Adresse des MMB ändern wollen, führen Sie das SNMP-Kommando für Sicherheitseinstellungen (setsnmpsec) aus. Näheres über dieses Kommando finden Sie im Handbuch *PRIMEQUEST 500A/500/400 Series Reference Manual: Basic Operation/GUI/Commands* (U41633-J-Z816-x-76/C122-E003EN).

5 WMI-Einstellungen (Window Management Instrumentation)
  PSA sammelt mithilfe von WMI, das in Windows standardmäßig installiert ist, Informationen zu PCI-Karten und SCSI-Geräten.
  Wenn der Speicherplatz und die Anzahl interner Handles, die WMI ausführt, um diese Informationen zu sammeln, für die Anzahl der vorhandenen LUNs (z.B. RAIDS) nicht ausreichen, dann ändern Sie die Einstellungen wie folgt:

- Maximaler Speicherplatz: 536.870.912 Byte
- Maximale Anzahl interner Handles: 65.536

6) Task Scheduler-Einstellungen

Nehmen Sie die folgenden Task Scheduler-Einstellungen vor, um die Stromversorgung der Expansion File Unit und die Lüfter auf Fehler zu überwachen:

Task-Name: File Unit Status Check

Aktivierungsintervall: 5 Minuten

Die Konfigurationsinformationen werden beim PSA-Start aufgenommen. Die Fehlererfassung wird anschließend auf dieser Grundlage bis zum nächsten PSA-Start ausgeführt. Ist keine Expansion File Unit angeschlossen, wird die Überwachung gemäß der Scheduler-Einstellung gestartet, jedoch sofort ohne weitere Erfassungsmaßnahmen eingestellt. Hierdurch wird das System nicht belastet.

Hinweise:

- Wenn Sie das PSA-Fenster nach der Installation mit anschließendem Neustart des Systems zum ersten Mal über das Web-UI öffnen wollen, erscheint möglicherweise die Fehlermeldung „E_33077 PSA is Not Active. (01:0000)“. Das liegt daran, dass der PSA einige Zeit benötigt, um Sensordaten vom System zu erhalten. Warten Sie einige Minuten und versuchen Sie dann erneut, das Fenster zu öffnen.
- Wenn Sie die IP-Adresse des MMBs oder des Management-LANs geändert haben, müssen Sie den PSA unbedingt neu starten. Andernfalls kommt es zu einem Anzeigefehler im Web-UI und erkennbare Fehler können im PSA nicht gemeldet werden.
- Folgendes ist bei der Einrichtung des PSA in Windows zu beachten:
  - Aktivieren Sie nicht die Option Visual Notification unter Dr. Watson, da der PSA ansonsten bei Auftreten eines Fehlers mit Anzeige eines Meldungsfensters nicht neu gestartet werden kann, bis das Fenster geschlossen wurde.
  - Setzen Sie bei den Eigenschaften für das Systemlog des Event Viewer nicht die Option „Do not overwrite events (clear log manually)**“**, da ansonsten ein Fehler nicht mehr in die Logdatei geschrieben wird, wenn diese ihre maximale Größe erreicht hat.

- Stoppen Sie nicht den Windows Print Spooler Service.
  Die Erfassungsfunktion des Betriebssystems verwendet die Windows Management Instrumentation (WMI). Wenn der Print Spooler Service gestoppt wird, wird dem WMI ein Fehler gemeldet, und die Konfigurationsinformationen können nicht mehr korrekt erfasst werden.

[Beginn der Ergänzung gemäß Handbuch-Errata 2006/10/10]

- Falls der folgende Wert in der Registry auf unter 20000 (dies bedeutet 20 Sekunden) eingestellt ist, kann das Windows-Betriebssystem möglicherweise beim Shutdown abstürzen. Deshalb muss der Wert unbedingt größer als 20000 (dies bedeutet 20 Sekunden) eingestellt werden. (Standard-Voreinstellung: 20000)
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WaitToKillServiceTimeout
  (Dieser Registry-Wert legt fest, wie lange das System nach dem Windows-Shutdown wartet, bevor die Services gestoppt werden.)
- Beim PSA-Start wird möglicherweise die folgende Meldung angezeigt, die jedoch keinerlei Probleme verursacht:
  „PM child process abnormal end [6:750] (tagt) 1:0x00000000“
  FJSVpsa Event ID 62

[Ende der Ergänzung gemäß Handbuch-Errata 2006/10/10]

4.5.1 Einstellungen für das Management-LAN überprüfen

Dieser Abschnitt beschreibt, wie Sie die Einstellungen für das Management-LAN überprüfen können.
Damit der PSA über das Management-LAN mit dem MMB kommunizieren kann, muss die partitionsseitig mit dem Management-LAN verbundene NIC aktiviert sein.

Hinweis: Konfigurieren Sie das Management-LAN erst nach Abschluss der Installation, wenn Sie die Installation mit dem Batch Installer der High Reliability Tools durchführen.

(1) NIC des Management-LANs ermitteln

Zeigen Sie im Device Manager die Eigenschaften der dem Management-LAN zugewiesenen Netzwerkadapter (Intel PRO/100 VE Network Connection und Intel PRO/100 M Network Connection) an und überprüfen Sie die Einstellungen für [Location] auf dem Registerblatt [General].

Schließen Sie die Netzwerkadapter für das Management-LAN wie folgt an MMB 0 und MMB 1 an:

- MMB 0: PCI-Bus 1, Device 8, Funktion 0
- MMB 1: PCI-Bus 1, Device 0, Funktion 0

Konfigurieren Sie die oben genannten Netzwerkadapter mit der Teaming-Funktion von Intel PROSet für eine duplizierte Kommunikation mit dem Management-LAN.

Geben Sie für das Intel PROSet-Teaming die IP-Adressen der Geräte für das Management-LAN an, die für die duplizierte Kommunikation konfiguriert sind.

(2) Netzwerkadapter des Management-LANs duplizieren

Benutzen Sie die Teaming-Funktion von Intel PROSet, um die Netzwerkadapter für das Verwaltungs-LAN so zu konfigurieren, dass duplizierte Kommunikationswege gewährleistet sind.

Installieren Sie dafür zuerst Intel PROSet.

Hinweise:

- Ändern Sie die VLAN-Einstellung der Management-LAN-Schnittstelle des MMB zu „VLAN Mode“. (Näheres finden Sie unter 2.2.4.5, „Einen Management-LAN-Hub einrichten“.)
- Auf dem Switch, der mit dem Benutzerport (Management-LAN) des MMB verbunden ist, muss SPT (Spanning Tree-Protokoll) deaktiviert sein.
- Es muss eine Verbindung zur Konsole hergestellt werden, um die Einstellungen über eine Verbindung zum entfernten Desktop durchführen zu können. Stellen Sie diese Verbindung wie folgt her:

  1) Wählen Sie im [Start]-Menü [Run] aus. Das Dialogfenster [Run] wird geöffnet.
  2) Geben Sie im Eingabefeld [Open] „mstsc /v:<servername/ip address> /console“ ein und klicken Sie auf [OK].

  Anm.: Die Teaming-Funktion ändert möglicherweise die IP-Adresse des Management-LANs, weil es als neues Device identifiziert wird. Eine Verbindung von einem entfernten System zum Management-LAN kann dabei abgebrochen werden.

  Stellen Sie in diesem Fall eine Verbindung über ein KVM-Gerät unter Eingabe der richtigen IP-Adresse her.

Geben Sie als Serververbindung einen aktuellen Servernamen und dessen IP-Adresse im Format <servername/ip address> ein. (Es kann keine virtuelle IP-Adresse des Clusters angegeben werden.)

* Nähere Einzelheiten über die Optionen von mstsc können Sie erfahren, indem Sie „mstsc /?“ eingeben.

1 Wählen Sie [Control Panel] → [Administrative Tools] → [Computer Management] → [Device Manager].

2 Öffnen Sie [Network Adapter] und wählen Sie [Inter(R) PRO/100 VE Network Connection].

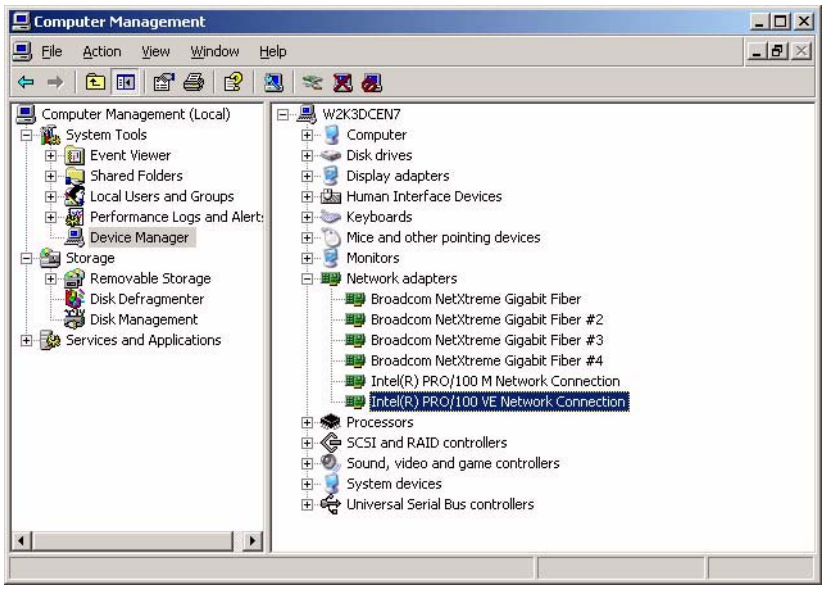


Abbildung 4.15 Fenster [Computer Management]

3 Das Dialogfenster [Intel(R) PRO/100 VE Network Connection Properties] wird angezeigt.
Wählen Sie das Registerblatt [Teaming] aus, aktivieren Sie das Optionsfeld [Team with other adapters] und klicken Sie auf die Schaltfläche [New Team].

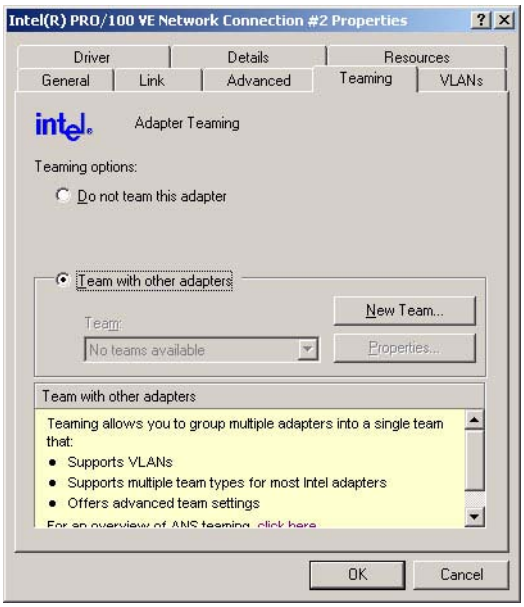


Abbildung 4.16 Registerblatt [Teaming]

4 Der [New Team Wizard] wird angezeigt. Geben Sie einen Teamnamen ein (Standardname ist Team #n) und klicken Sie auf [Next].

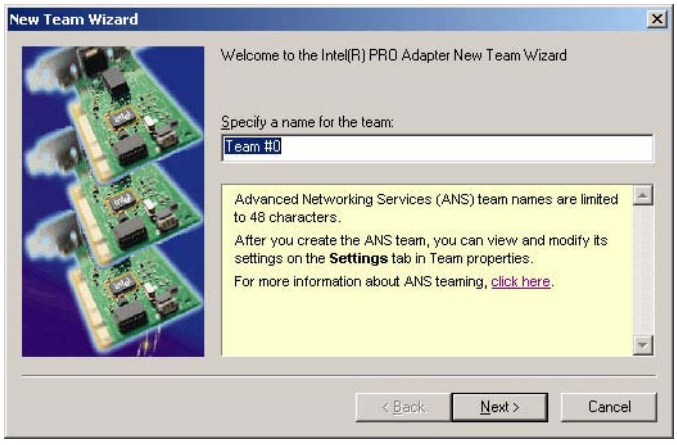

New Team Wizard
Welcome to the Intel(R) PRO Adapter New Team Wizard
Specify a name for the team:
Team #0
Advanced Networking Services (ANS) team names are limited to 48 characters.
After you create the ANS team, you can view and modify its settings on the Settings tab in Team properties.
For more information about ANS teaming, click here.
< Back
Next >
Cancel

Abbildung 4.17 Dialogfenster [New Team Wizard]

5 Eine Liste der für das Teaming verfügbaren Netzwerkadapter wird angezeigt. Aktivieren Sie die Kontrollkästchen für [Intel(R) PRO/100 VE Network Connection] und [Intel(R) Pro/100 M Network Connection] und klicken Sie auf [Next].

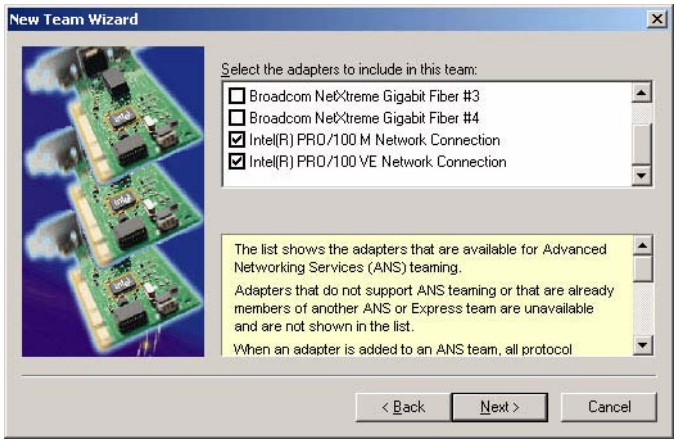

New Team Wizard
Select the adapters to include in this team:
Broadcom NetXtreme Gigabit Fiber #3
Broadcom NetXtreme Gigabit Fiber #4
Intel(R) PRO/100 M Network Connection
Intel(R) PRO/100 VE Network Connection
The list shows the adapters that are available for Advanced Networking Services (ANS) teaming.
Adapters that do not support ANS teaming or that are already members of another ANS or Express team are unavailable and are not shown in the list.
When an adapter is added to an ANS team, all protocol
< Back
Next >
Cancel

Abbildung 4.18 Liste der Netzwerkadapter

6 Wählen Sie in der Modusliste [Adapter Fault Tolerance] aus und klicken Sie auf [Next].

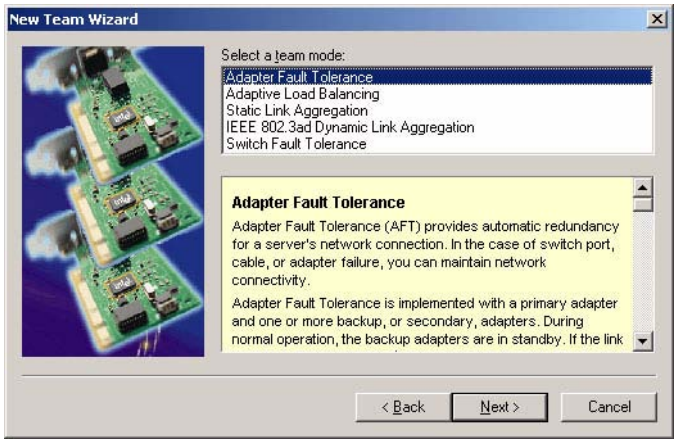

New Team Wizard
Select a team mode:
Adapter Fault Tolerance
Adaptive Load Balancing
Static Link Aggregation
IEEE 802.3ad Dynamic Link Aggregation
Switch Fault Tolerance
Adapter Fault Tolerance
Adapter Fault Tolerance (AFT) provides automatic redundancy for a server's network connection. In the case of switch port, cable, or adapter failure, you can maintain network connectivity.
Adapter Fault Tolerance is implemented with a primary adapter and one or more backup, or secondary, adapters. During normal operation, the backup adapters are in standby. If the link
< Back
Next >
Cancel

Abbildung 4.19 Team-Modus-Liste

7 Das folgende Fenster erscheint. Die Einrichtung des Teaming beginnt, wenn Sie auf [Finish] klicken.

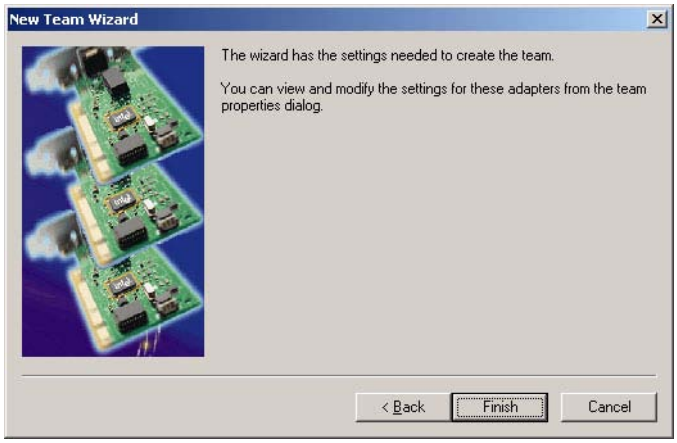

New Team Wizard
The wizard has the settings needed to create the team.
You can view and modify the settings for these adapters from the team properties dialog.
< Back
Finish
Cancel

Abbildung 4.20 Auswahl abgeschlossen

8 Wenn die Konfigurierung des Teaming abgeschlossen ist, ist das Teaming-Gerät angelegt und die Eigenschaften des Teams werden angezeigt.
Klicken Sie das Register [Settings] an und überprüfen Sie die angezeigten Adapterinformationen. Wenn die Angaben korrekt sind, klicken Sie auf [OK]. Andernfalls klicken Sie auf [Remove Team], um das Teaming-Gerät zu entfernen. Führen Sie den beschriebenen Vorgang in dem Fall ab Schritt 2 noch einmal durch.

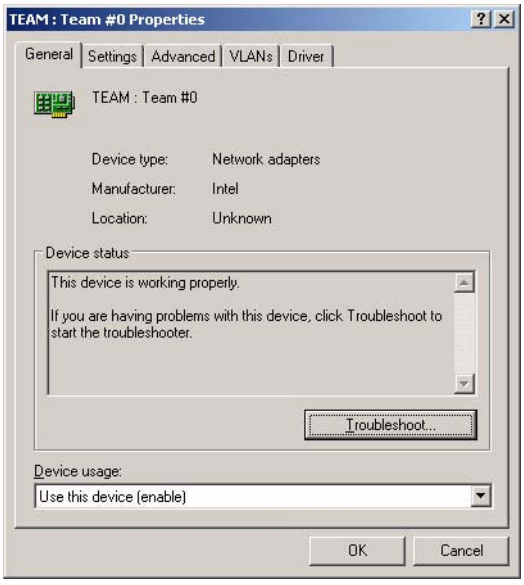


Abbildung 4.21 Eigenschaften des Teams Nummer 0

9 Das Dialogfenster [Intel(R) PRO/100 VE Network Connection Properties] wird wieder angezeigt.
Klicken Sie auf [OK], um den Vorgang zu beenden und schließen Sie [Computer Management].

10 Wählen Sie [Control Panel] und [Network Connections].
Es wird eine Liste der Netzwerke angezeigt.

11 Wählen Sie das Netzwerk, dessen Gerätename dem Teamnamen entspricht (z.B. Team #0) und wählen Sie aus dem Kontextmenü den Eintrag [Properties] aus.

12 Wählen Sie [Internet Protocol (TCP/IP)], klicken Sie auf die Schaltfläche [Properties] und geben Sie im Dialogfenster [Internet Protocol (TCP/IP) Properties] die IP-Adresse, die Teilnetzmaske, das Standard-Gateway und sonstige Parameters ein.

13 Klicken Sie auf [Configure], um die Eigenschaften des Teams anzuzeigen.

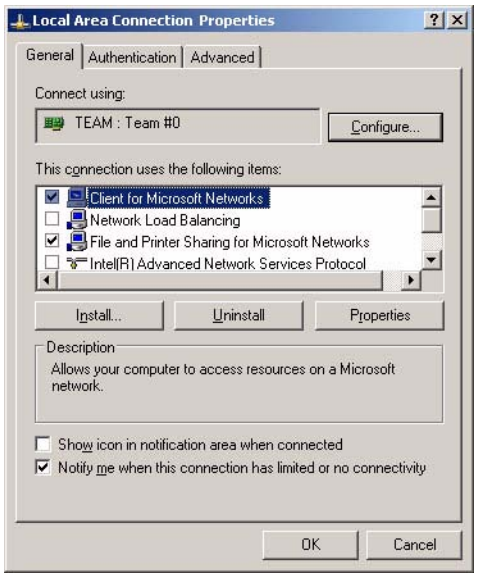


Abbildung 4.22 Dialogfenster [Local Area Connection Properties]

14 Wählen Sie auf dem Registerblatt [Advanced] unter [Settings] den Eintrag [Probe] aus und aus der Dropdown-Liste unter [Value] die Option [Enable]. Klikken Sie auf [OK], um die Eingaben zu bestätigen.
Der Adapter aktiviert daraufhin die Verbindungsüberwachung und die Duplizierung des Management-LANs ist somit eingestellt.
Führen Sie einen Neustart aus, damit die Teaming-Einstellungen wirksam werden.

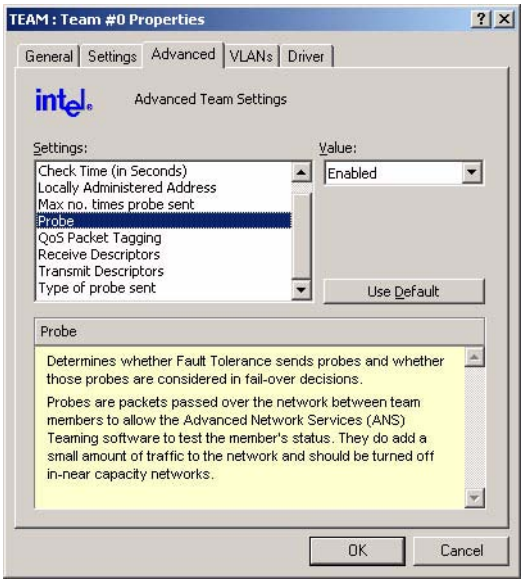

TEAM : Team #0 Properties
General
Settings
Advanced
VLANs
Driver
Advanced Team Settings
Settings:
Value:
Check Time (in Seconds)
Locally Administered Address
Max no. times probe sent
Probe
QoS Packet Tagging
Receive Descriptors
Transmit Descriptors
Type of probe sent
Enabled
Use Default
Probe
Determines whether Fault Tolerance sends probes and whether those probes are considered in fail-over decisions.
Probes are packets passed over the network between team members to allow the Advanced Network Services (ANS) Teaming software to test the member's status. They do add a small amount of traffic to the network and should be turned off in-near capacity networks.
OK
Cancel

Abbildung 4.23 Registerblatt [Advanced]

4.5.2 Ziel für Partition-Traps einstellen

Hinweise:

- SNMP V.3 wird von Windows nicht unterstützt.
- Führen Sie diese Aufgaben nur durch, wenn die Einstellung gebraucht wird.
- Die Einstellungen sind erforderlich, wenn Partitionen mit einer Betriebsverwaltungssoftware verwaltet werden.

1 Wählen Sie [Control Panel] → [Administrative Tools].

2 Wählen Sie [Computer Management].

3 Wählen Sie in der Baumstruktur links [Services and Applications] → [Services].

4 Klicken Sie im rechten Teilfenster [SNMP Service] an.
Das Dialogfenster [SNMP Service] wird angezeigt.

5 Klicken Sie auf das Registerblatt [Trap].

6 Geben Sie im Feld [Community Name] den Namen der gewünschten Community ein und klicken Sie auf [Add to List].

7 Klicken Sie unter [Trap Send Destination] auf [Add].

8 Geben Sie den Hostnamen oder die IP-Adresse des Servers ein, an den die Traps zur Benachrichtigung geschickt werden und klicken Sie auf [Add].

9 Klicken Sie dann auf [OK].

10 Wählen Sie im Menü [Action] den Eintrag [Restart], um den SNMP-Dienst neu zu starten.

Einstellungen für Trap-Ziel überprüfen

Benutzen Sie die Standard-Trap des SNMP-Dienstes, die in Schritt 10 des SNMP-Service-Neustarts zum Einsatz kommt, um zu überprüfen, ob die Einstellungen für das Trap-Ziel richtig sind. Stellen Sie sicher, dass die Traps ordnungsgemäß am gewünschten Ziel empfangen werden.

Anm.: Auf dem Zielrechner muss eine Trap-Anwendung oder ein Trap Manager aktiviert sein, damit die Traps des SNMP-Dienstes empfangen werden können.

Starten Sie den SNMP-Dienst auf dem Ausgangsrechner neu, indem Sie Schritt 10 durchführen.

Als Ergebnis erhält die Trap-Anwendung auf dem Zielrechner die Standardmeldung „ColdStart“.

Handelt es sich beispielsweise bei dem Zielrechner um einen Linux-Rechner, wird die folgende Meldung in die Datei syslog geschrieben, wenn snmptrapd eine Trap erhält. Das zeigt, dass das Zielgerät Traps ordnungsgemäß empfängt.

Aug 17 14:50:03 shaka snmptrapd[2600]: 2005-08-17 14:50:03 pq-server.fujitsu.com [192.168.0.162] (via 192.168.0.162) TRAP, SNMP v1, community public SNMPv2-SMI::enterprises.211.1.31.1.2.100.3 Cold Start Trap (0) Uptime: 0:00:00.00

4.5.3 Ziel für Traps und E-Mails über MMB festlegen

Hinweise:

- Machen Sie diese Einstellung nur, wenn sie erforderlich ist.
- Die Einstellung ist erforderlich, wenn Partitionen mit einer Betriebsverwaltungssoftware verwaltet werden.

Das Ziel für Trap- und E-Mail-Übertragungen über MMB kann mit der MMB Web-UI eingestellt werden.

Näheres über das MMB Trap-Ziel finden Sie in Abschnitt 5.1.2, „SNMP einrichten“. Näheres über das E-Mail-Ziel finden Sie in Abschnitt 2.2.3.5, „SMTP-Einstellungen“.

4.5.4 Windows-Firewall einstellen

Wenn Sie die Windows-Firewall benutzen wollen, müssen Sie über [Exceptions] sicherstellen, dass eine Datenübertragung zum MMB über die folgenden Ports gewährleistet ist:

- TCP-Port, der vom PSA benutzt wird: Port 24450
- UDP-Port, der für SNMP benötigt wird: Port 161

1 Wählen Sie [Control Panel] → [Windows Firewall].
Das Fenster [Windows Firewall] wird angezeigt.

2 Wählen Sie das Registerblatt [Exceptions] und klicken Sie dort auf die Schaltfläche [Add Port].
Das Dialogfenster [Add Port] wird geöffnet.

3 Geben Sie die Nummer des vom PSA benutzten Ports ein und klicken Sie auf [OK].

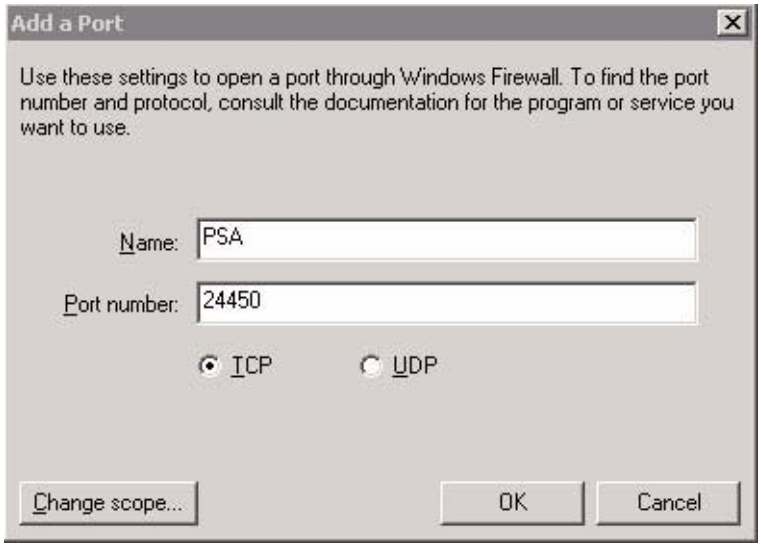


Abbildung 4.24 Dialogfenster [Add a Port]

4 Klicken Sie im Fenster [Windows Firewall] noch einmal auf die Schaltfläche [Add Port].
Das Dialogfenster [Add Port] wird geöffnet.

5 Geben Sie die Nummer des von SNMP benutzten Ports ein und klicken Sie auf [OK].

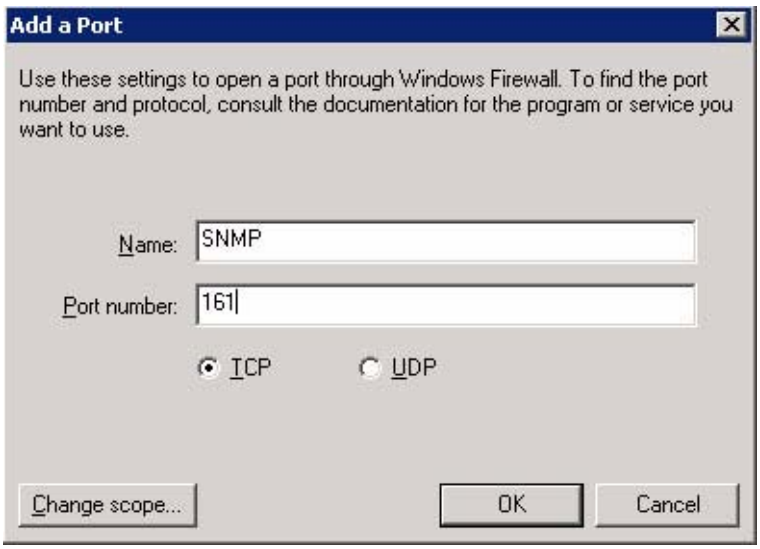


Abbildung 4.25 Dilaogfenster [Add a Port]

6 Klicken Sie im Fenster [Windows Firewall] auf die Schaltfläche [OK], um die Einstellungen abzuschließen.

4.5.5 Watchdog-Überwachung nach Auftreten eines Stopp-Fehlers (eines schwerwiegenden Systemfehlers)

Tritt im System ein Stopp-Fehler (ein schwerwiegender Systemfehler) auf, passiert Folgendes:

- Unter „System Progress“ der entsprechenden Partition unter [Partition]-[Power Control] des MMB Web-UI wird „Panic“ ausgegeben.
- Ein Speicherabzug (Memory dump) des Systems wird erstellt.

Um in solchen Fällen zu verhindern, dass das System einfriert oder anderweitig nicht mehr antwortet, kann eine Überwachung mithilfe des Watchdog-Timers eingestellt werden.

Nach Ablauf der eingestellten Zeit führt MMB einen harten Reset aus, und das Betriebssystem wird neu gestartet.

Einstellungsablauf

1 Öffnen Sie folgende Datei:
PSA Installationsordner: \etc\opt\FJSVpsa\usr\pnwatchdog.conf
(Beispiel: C:\Program Files\fujitsu\FJSVpsa\etc\opt\FJSVpsa\usr \pnwatchdog.conf)

2 Geben Sie, wie unten dargestellt, einen Schlüsselwert ein. Standard ist 0.
Abschnitt: [WATCHDOG]
Schlüssel: [TIMER]
Wert einstellen (Einheit: Sekunden)0 (Watchdog-Timer wird nicht benutzt)
1 bis 6000 (Überwachungszeitraum des Watchdog-Timers)

Anm.: Zur Einstellung des Werts messen Sie die benötigte Zeit für einen Speicherabzug in der maßgeblichen Partition und bestimmen den entsprechenden Wert. Übersteigt die benötigte Zeit 6000 Sekunden (1 Stunde und 40 Minuten), geben Sie 0 an (Watchdog-Timer wird nicht benutzt).
Ist der eingestellte Zeitraum kürzer als die benötigte Zeit für die Erstellung des Speicherabzugs, läuft die Zeit für den Watchdog-Timer ab, was zu einem harten Reset führt. Der Speicherabzug kann nicht mehr ordnungsgemäß abgeschlossen werden.

4.5.6 PSA-Updates installieren

In diesem Abschnitt wird beschrieben, wie Sie ein PSA-Update installieren.

Anm.: Wenden Sie sich an Ihren Kundendienst-Techniker oder an das Support Center, um zu erfahren, wie Sie Fix-Programme erhalten.

Hinweis: Ist PEXU gemountet, benutzen Sie PSA ab Version 1.10.

(1) Kleinere Updates installieren

1 Speichern Sie das Fix-Programm (fjpsaxxxx.exe) im gewünschten Ordner.

2 Starten Sie das Fix-Programm. Der folgende Bildschirm zeigt an, dass die Installation vorbereitet wird:

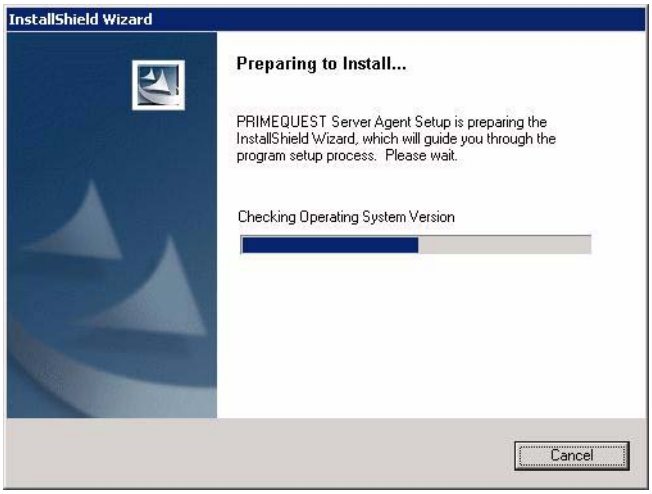

InstallShield Wizard
Preparing to Install...
PRIMEQUEST Server Agent Setup is preparing the InstallShield Wizard, which will guide you through the program setup process. Please wait.
Checking Operating System Version
Cancel

Abbildung 4.26 Installationsvorbereitung

3 Klicken Sie auf die Schaltfläche [Next], um die Installation auszuführen, wenn der folgende Bildschirm anzeigt, dass das System für die Installation bereit ist. Die Aktualisierung des Programms beginnt.

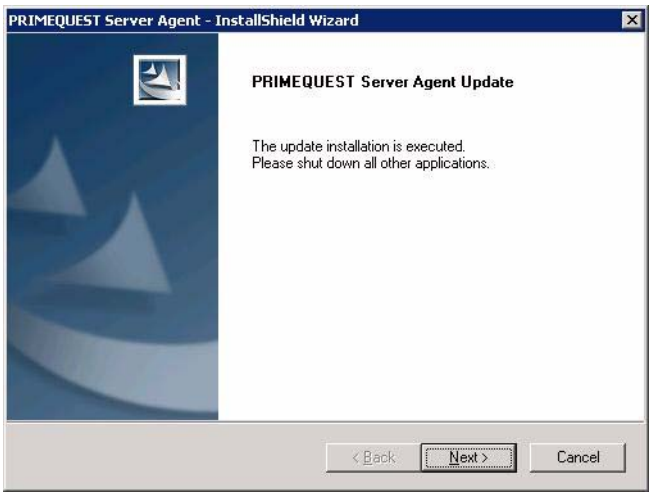

PRIMEQUEST Server Agent - InstallShield Wizard
PRIMEQUEST Server Agent Update
The update installation is executed.
Please shut down all other applications.
< Back
Next >
Cancel

Abbildung 4.27 Update-Installation

4 Klicken Sie auf die Schaltfläche [Finish], um den Vorgang abzuschließen.

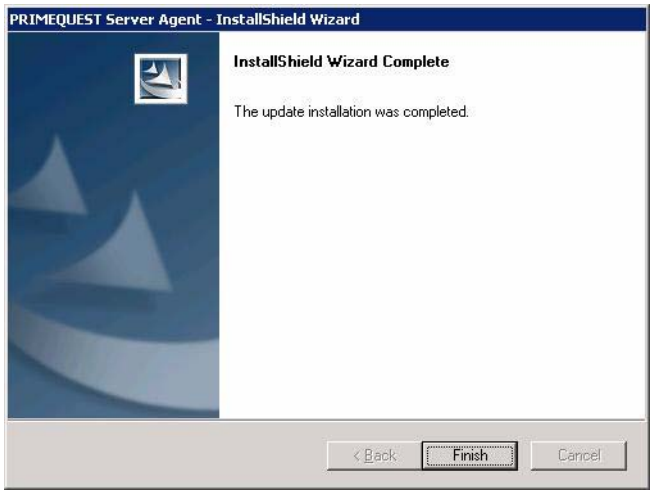


Abbildung 4.28 Update abgeschlossen

5 Wenn ein Neustart erforderlich ist, werden Sie in einem Dialogfeld gefragt, ob der Neustart durchgeführt werden soll. Überprüfen Sie, ob ein Neustart zum gegebenen Zeitpunkt problemlos durchgeführt werden kann und starten Sie das System dann neu, indem Sie auf die Schaltfläche [Finish] klicken.

(2) Umfangreichere Updates installieren

1 Speichern Sie das Fix-Programm (fjpsaxxxx.exe) im gewünschten Ordner.

2 Starten Sie das Fix-Programm. Der folgende Bildschirm zeigt an, dass die Installation vorbereitet wird:

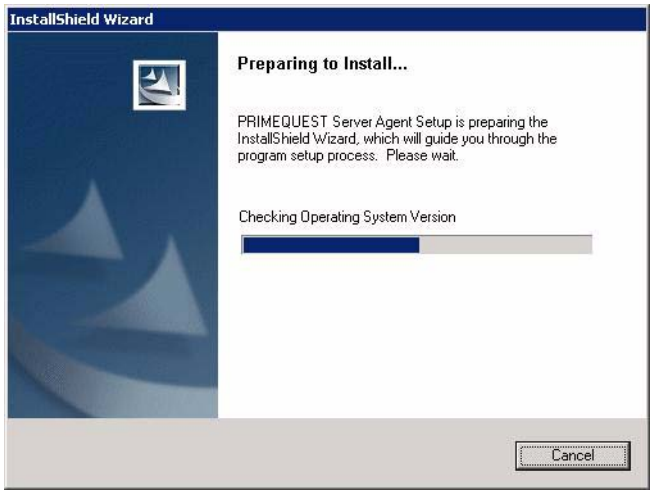

InstallShield Wizard
Preparing to Install...
PRIMEQUEST Server Agent Setup is preparing the InstallShield Wizard, which will guide you through the program setup process. Please wait.
Checking Operating System Version
Cancel

Abbildung 4.29 Installationsvorbereitung

3 Klicken Sie auf die Schaltfläche [OK], wenn das Bestätigungsfenster erscheint. Die Deinstallation wird daraufhin gestartet.

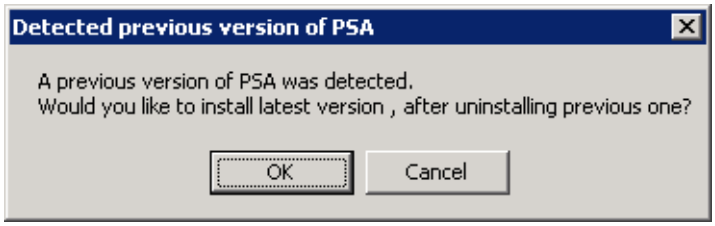

Detected previous version of PSA
A previous version of PSA was detected.
Would you like to install latest version , after uninstalling previous one?
OK
Cancel

Abbildung 4.30 [Detected previous version of PSA]

4 Wenn die Deinstallation abgeschlossen ist, wird die Installation der neuen Version gestartet.

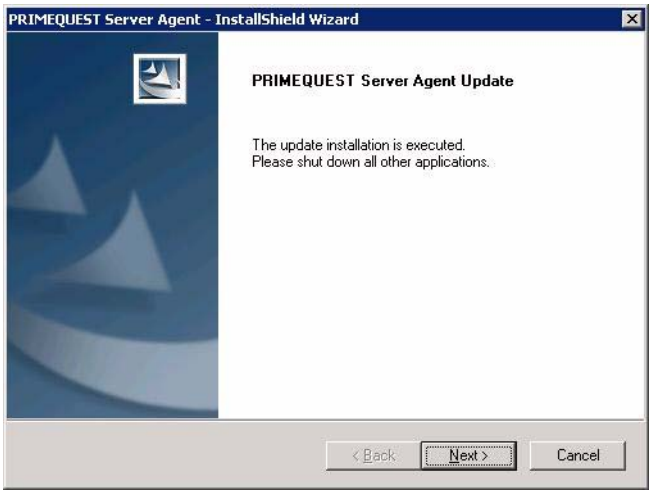

PRIMEQUEST Server Agent - InstallShield Wizard
PRIMEQUEST Server Agent Update
The update installation is executed.
Please shut down all other applications.
< Back
Next >
Cancel

Abbildung 4.31 Update-Installation

5 Geben Sie das Installationsziel an und klicken Sie dann auf die Schaltfläche [Next]. Die neue Version wird standardmäßig im Ordner „Program Files\Fujitsu“ installiert. Wenn Sie ein anderes Installationsziel bestimmen wollen, klicken Sie auf die Schaltfläche [Browse] und geben Sie das gewünschte Ziel an.

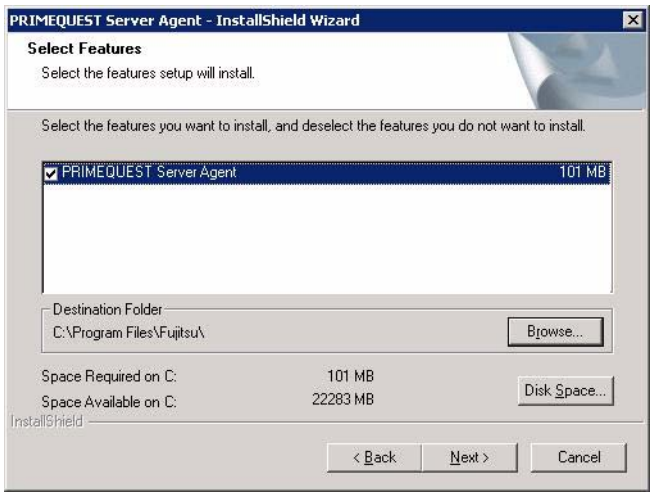


Abbildung 4.32 Fenster [Select Features]

6 Wenn die Installation abgeschlossen ist, wird das folgende Bestätigungsfenster angezeigt. Klicken Sie auf die Schaltfläche [Finish].

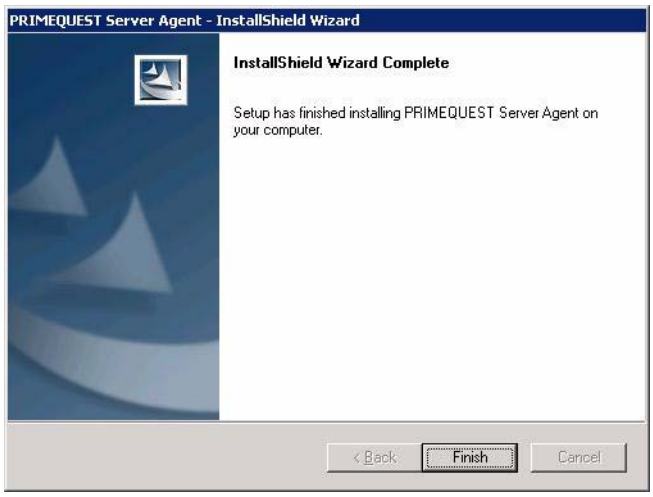


Abbildung 4.33 Installation abgeschlossen

7 Wenn ein Neustart erforderlich ist, werden Sie in einem Dialogfeld gefragt, ob der Neustart durchgeführt werden soll. Überprüfen Sie, ob ein Neustart zum gegebenen Zeitpunkt problemlos durchgeführt werden kann und starten Sie das System dann neu, indem Sie auf die Schaltfläche [Finish] klicken.

4.5.7 PSA deinstallieren

In diesem Abschnitt wird beschrieben, wie Sie PSA deinstallieren.

1 Wählen Sie [Control Panel] → [Add/Remove Programs] aus.

2 Wählen Sie unter [Currently Installed Programs] den Eintrag [PRIMEQUEST Server Agent] aus und klicken Sie auf die Schaltfläche [Change/Delete].

3 Sie werden aufgefordert, die Deinstallation zu bestätigen. Klicken Sie auf [OK], um die Deinstallation zu starten.

Abbildung 4.34 Bestätigungsfenster

4 Wenn die Deinstallation abgeschlossen ist, erscheint das folgende Bestätigungsfenster. Klicken Sie auf die Schaltfläche [Finish].

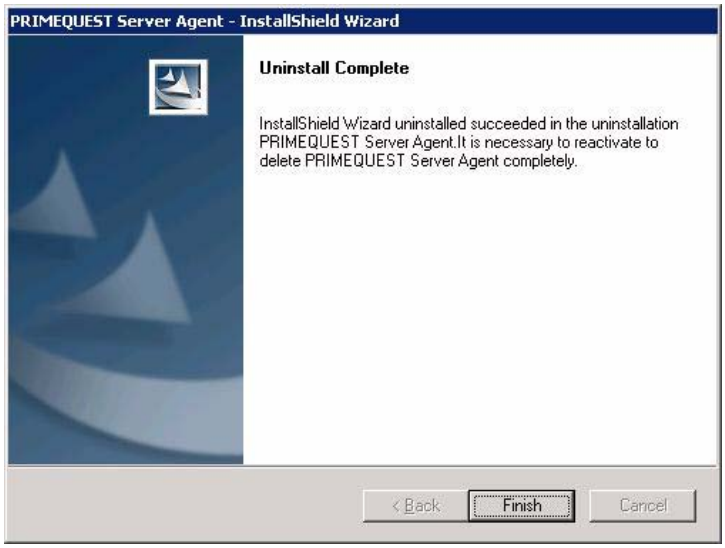

PRIMEQUEST Server Agent - InstallShield Wizard
Uninstall Complete
InstallShield Wizard uninstalled succeeded in the uninstallation PRIMEQUEST Server Agent.It is necessary to reactivate to delete PRIMEQUEST Server Agent completely.
< Back
Finish
Cancel

Abbildung 4.35 Deinstallation abgeschlossen

5 Wenn ein Neustart erforderlich ist, werden Sie in einem Dialogfeld gefragt, ob der Neustart durchgeführt werden soll. Überprüfen Sie, ob ein Neustart zum gegebenen Zeitpunkt problemlos durchgeführt werden kann und starten Sie das System dann neu, indem Sie auf die Schaltfläche [Finish] klicken.

4.6 PSA installieren (Windows Server 2003) (PRIMEQUEST 520A*/520/420)

In diesem Abschnitt wird die Installation des PSA beschrieben.

Obligatorische Aufgaben:

- Einstellungen für das Management-LAN überprüfen (→ 4.6.1)

Optionale Aufgaben:

- Ziel für Partition-Traps einstellen (→ 4.6.2)
- Ziel für Traps und E-Mails über MMB festlegen (→ 4.6.3)
- Windows-Firewall einstellen (→ 4.6.4)
- Watchdog-Überwachung nach Auftreten eines Stopp-Fehlers (eines schwerwiegenden Systemfehlers) (→ 4.6.5)

Anm.:

- Benutzen Sie den PRIMEQUEST Software Installer oder Systemcast-Wizard Lite, um den PSA zu installieren. Wie Sie den PSA manuell installieren können, ist in Kapitel 4, „Manual PSA Installation“ im *PRIMEQUEST 500A/500/400 Series Reference Manual: Tools/Operation Information* (U41757-J-Z816-x-76/C122-E074EN) beschrieben. Näheres über eine Installation mit dem PRIMEQUEST Software Installer finden Sie in Abschnitt 3.3.6.1, „Installation mit PRIMEQUEST Software Installer“.
  Die Installation mit SystemcastWizard Lite ist im *PRIMEQUEST SystemcastWizard Lite User's Guide* (C122-E010EN) beschrieben.
- Bei der Installation des PSA werden die folgenden für den Betrieb erforderlichen Einstellungen automatisch durchgeführt:

1 Einstellung der Dienste
- PRIMEQUEST Server Agent
- PRIMEQUEST PEM Command Service
- PRIMEQUEST PSA Environment Control Service

2 Einstellung der Umgebungsvariablen
- Die Variable PATH
  Der von PSA zu verwendende Wert wird der bestehenden PATH-Variable hinzugefügt.

*: wird von Fujitsu Technology Solutions nicht unterstützt

- Variable FJSVpsa_INSTALLPATH
  Diese Variable wird neu hinzugefügt.

3 Port-Einstellung
  Es wird damit sichergestellt, dass PSA den Port TCP:24450 verwendet.

4 SNMP-Sicherheitseinstellungen
  Machen Sie die erforderlichen Sicherheitseinstellungen für den SNMP-Dienst, da der PSA vom MMB SNMP-Pakete empfangen muss.
  Die weitere Vorgehensweise hängt von dem Parameter ab, der während der Installation des PSA auf dem Registerblatt [Security] des Fensters [Properties] für [SNMP Service] ausgewählt wird.

- Wenn [Accept SNMP packets from any host] ausgewählt wird:
  SNMP-Sicherheitseinstellungen sind nicht erforderlich.
- Wenn [Accept SNMP packets from these hosts] ausgewählt wird:
  Richten Sie mit Ihren Einstellungen eine sichere SNMP-Übertragung ein, wenn die IP-Adresse des MMB und der Parameter für den lokalen Host nicht angegeben sind.

  Hinweis: Wenn Sie die Einstellung nach der Installation des PSA von [Accept SNMP packets from any host] in [Accept SNMP packets from these hosts] ändern wollen oder wenn Sie die IP-Adresse des MMB ändern wollen, führen Sie das SNMP-Kommando für Sicherheitseinstellungen (setsnmpsec) aus. Näheres über dieses Kommando finden Sie im Handbuch *PRIMEQUEST 500A/500/400 Series Reference Manual: Basic Operation/GUI/Commands* (U41633-J-Z816-x-76/C122-E003EN).

5 WMI-Einstellungen (Window Management Instrumentation)
  PSA sammelt mithilfe von WMI, das in Windows standardmäßig installiert ist, Informationen zu PCI-Karten und SCSI-Geräten.
  Wenn der Speicherplatz und die Anzahl interner Handles, die WMI ausführt, um diese Informationen zu sammeln, für die Anzahl der vorhandenen LUNs (z.B. RAIDS) nicht ausreichen, dann ändern Sie die Einstellungen wie folgt:

- Maximaler Speicherplatz: 536.870.912 Byte
- Maximale Anzahl interner Handles: 65.536

6) Task Scheduler-Einstellungen

Nehmen Sie die folgenden Task Scheduler-Einstellungen vor, um die Stromversorgung der Expansion File Unit und die Lüfter auf Fehler zu überwachen:

Task-Name: File Unit Status Check

Aktivierungsintervall: 5 Minuten

Die Konfigurationsinformationen werden beim PSA-Start aufgenommen. Die Fehlererfassung wird anschließend auf dieser Grundlage bis zum nächsten PSA-Start ausgeführt. Ist keine Expansion File Unit angeschlossen, wird die Überwachung gemäß der Scheduler-Einstellung gestartet, jedoch sofort ohne weitere Erfassungsmaßnahmen eingestellt. Hierdurch wird das System nicht belastet.

Hinweise:

- Wenn Sie das PSA-Fenster nach der Installation mit anschließendem Neustart des Systems zum ersten Mal über das Web-UI öffnen wollen, erscheint möglicherweise die Fehlermeldung „E_33077 PSA is Not Active. (01:0000)“. Das liegt daran, dass der PSA einige Zeit benötigt, um Sensordaten vom System zu erhalten. Warten Sie einige Minuten und versuchen Sie dann erneut, das Fenster zu öffnen.
- Wenn Sie die IP-Adresse des MMBs oder des Management-LANs geändert haben, müssen Sie den PSA unbedingt neu starten. Andernfalls kommt es zu einem Anzeigefehler im Web-UI und erkennbare Fehler können im PSA nicht gemeldet werden.
- Folgendes ist bei der Einrichtung des PSA in Windows zu beachten:
  - Aktivieren Sie nicht die Option Visual Notification unter Dr. Watson, da der PSA ansonsten bei Auftreten eines Fehlers mit Anzeige eines Meldungsfensters nicht neu gestartet werden kann, bis das Fenster geschlossen wurde.
  - Setzen Sie bei den Eigenschaften für das Systemlog des Event Viewer nicht die Option „Do not overwrite events (clear log manually)**“**, da ansonsten ein Fehler nicht mehr in die Logdatei geschrieben wird, wenn diese ihre maximale Größe erreicht hat.

- Stoppen Sie nicht den Windows Print Spooler Service.
  Die Erfassungsfunktion des Betriebssystems verwendet die Windows Management Instrumentation (WMI). Wenn der Print Spooler Service gestoppt wird, wird dem WMI ein Fehler gemeldet, und die Konfigurationsinformationen können nicht mehr korrekt erfasst werden.
- Falls der folgende Wert in der Registry auf unter 20000 (dies bedeutet 20 Sekunden) eingestellt ist, kann das Windows-Betriebssystem möglicherweise beim Shutdown abstürzen. Deshalb muss der Wert unbedingt größer als 20000 (dies bedeutet 20 Sekunden) eingestellt werden. (Standard-Voreinstellung: 20000)
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WaitToKillServiceTimeout
  (Dieser Registry-Wert legt fest, wie lange das System nach dem Windows-Shutdown wartet, bevor die Services gestoppt werden.)
- Beim PSA-Start wird möglicherweise die folgende Meldung angezeigt, die jedoch keinerlei Probleme verursacht:
  „PM child process abnormal end [6:750] (tagt) 1:0x00000000“ FJSVpsa Event ID 62

4.6.1 Einstellungen für das Management-LAN überprüfen

Dieser Abschnitt beschreibt, wie Sie die Einstellungen für das Management-LAN überprüfen können.
Damit der PSA über das Management-LAN mit dem MMB kommunizieren kann, muss die mit dem Management-LAN verbundene NIC aktiviert sein.

Hinweis: Konfigurieren Sie das Management-LAN erst nach Abschluss der Installation, wenn Sie die Installation mit dem Batch Installer der High Reliability Tools durchführen.

(1) NIC des Management-LANs überprüfen

Rufen Sie im Device Manager die Eigenschaften der dem Management-LAN zugewiesenen Netzwerkadapter (Intel PRO/100 VE Network Connection) auf und überprüfen Sie die Einstellungen für [Location] auf dem Registerblatt [General].

Schließen Sie die Netzwerkadapter für das Management-LAN wie folgt an das MMB an:

- MMB: PCI Bus 1, Device 8, Function 0

(2) Netzwerk-Adapter für das Management-LAN einstellen

Hinweise:

- Auf dem Switch, der mit dem Benutzerport (Management-LAN) des MMB verbunden ist, muss SPT (Spanning Tree-Protokoll) deaktiviert sein.
- Es muss eine Verbindung zur Konsole hergestellt werden, um die Einstellungen über eine Verbindung zum entfernten Desktop durchführen zu können. Stellen Sie diese Verbindung wie folgt her:

1 Wählen Sie im [Start]-Menü [Run] aus. Das Dialogfenster [Run] wird geöffnet.

2 Geben Sie im Eingabefeld [Open] „mstsc /v:<servername/ip address> /console“ ein und klicken Sie auf [OK].
Geben Sie als Serververbindung einen aktuellen Servernamen und dessen IP-Adresse im Format <servername/ip address> ein. (Es kann keine virtuelle IP-Adresse des Clusters angegeben werden.)
* Nähere Einzelheiten über die Optionen von mstsc können Sie erfahren, indem Sie „mstsc /?“ eingeben.

1 Wählen Sie [Control Panel] und [Network Connections] aus.
Es wird eine Liste der Netzwerke angezeigt.

2 Wählen Sie das Netzwerk aus, dessen Device-Name dem Team-Namen entspricht und wählen Sie im Kontextmenü den Eintrag [Properties] aus.

3 Wählen Sie [Internet Protocol (TCP/IP)] aus, klicken Sie auf die Schaltfläche [Properties] und geben Sie im Dialogfeld [Internet Protocol (TCP/IP) Properties] IP-Adresse, Teilnetzmaske, Standard-Gateway sowie sonstige Parameter ein.

4.6.2 Ziel für Partition-Traps einstellen

Hinweise:

- SNMP V.3 wird von Windows nicht unterstützt.
- Führen Sie diese Aufgaben nur durch, wenn die Einstellung gebraucht wird.
- Die Einstellungen sind für die Verbindung zu einer Betriebsverwaltungssoftware erforderlich.

1 Wählen Sie [Control Panel] → [Administrative Tools].

2 Wählen Sie [Computer Management].

3 Wählen Sie in der Baumstruktur links [Services and Applications] → [Services].

4 Klicken Sie im rechten Teilfenster [SNMP Service] an.
Das Dialogfenster [SNMP Service] wird angezeigt.

5 Klicken Sie auf das Registerblatt [Trap].

6 Geben Sie im Feld [Community Name] den Namen der gewünschten Community ein und klicken Sie auf [Add to List].

7 Klicken Sie unter [Trap Send Destination] auf [Add].

8 Geben Sie den Hostnamen oder die IP-Adresse des Servers ein, an den die Traps zur Benachrichtigung geschickt werden und klicken Sie auf [Add].

9 Klicken Sie dann auf [OK].

10 Wählen Sie im Menü [Action] den Eintrag [Restart], um den SNMP-Dienst neu zu starten.

Einstellungen für Trap-Ziel überprüfen

Benutzen Sie die Standard-Trap des SNMP-Dienstes, die bei dem in Schritt 10 genannten Neustart zum Einsatz kommt. Stellen Sie sicher, dass die Traps ordnungsgemäß am gewünschten Ziel empfangen werden.

Anm.: Auf dem Zielrechner muss eine Trap-Anwendung oder ein Trap Manager aktiviert sein, damit die Traps des SNMP-Dienstes empfangen werden können.

Starten Sie den SNMP-Dienst auf dem Ausgangsrechner neu, indem Sie Schritt 10 durchführen.

Die Trap-Anwendung auf dem Zielrechner erhält daraufhin die Standardmeldung „ColdStart“.

Handelt es sich beispielsweise bei dem Zielrechner um einen Linux-Rechner, wird die folgende Meldung in die Datei syslog geschrieben, wenn snmptrapd eine Trap erhält. Das zeigt, dass das Zielgerät Traps ordnungsgemäß empfängt.

Aug 17 14:50:03 shaka snmptrapd[2600]: 2005-08-17 14:50:03 pq-server.fujitsu.com [192.168.0.162] (via 192.168.0.162) TRAP, SNMP v1, community public SNMPv2-SMI::enterprises.211.1.31.1.2.100.3 Cold Start Trap (0) Uptime: 0:00:00.00

4.6.3 Ziel für Traps und E-Mails über MMB festlegen

Hinweise:

- Machen Sie diese Einstellung nur, wenn sie erforderlich ist.
- Die Einstellungen sind für die Verbindung zu einer Betriebsverwaltungssoftware erforderlich.

Das Ziel für Trap- und E-Mail-Übertragungen über MMB kann mit der MMB Web-UI eingestellt werden.

Näheres über das MMB Trap-Ziel finden Sie in Abschnitt 5.1.2, „SNMP einrichten“. Näheres über das E-Mail-Ziel finden Sie in Abschnitt 2.2.3.5, „SMTP-Einstellungen“.

4.6.4 Windows-Firewall einstellen

Wenn Sie die Windows-Firewall benutzen wollen, müssen Sie über [Exceptions] sicherstellen, dass eine Datenübertragung zum MMB über die folgenden Ports gewährleistet ist:

- TCP-Port, der vom PSA benutzt wird: Port 24450
- ~~**TCP**~~ **UDP**-Port, der für SNMP benötigt wird: Port 161

[Korrektur gemäß Handbuch-Errata 2009/02/24]

1. Wählen Sie [Control Panel] → [Windows Firewall].
   Das Fenster [Windows Firewall] wird angezeigt.
2. Wählen Sie das Registerblatt [Exceptions] und klicken Sie dort auf die Schaltfläche [Add Port].
   Das Dialogfenster [Add Port] wird geöffnet.
3. Geben Sie die Nummer des vom PSA benutzten Ports ein und klicken Sie auf [OK].

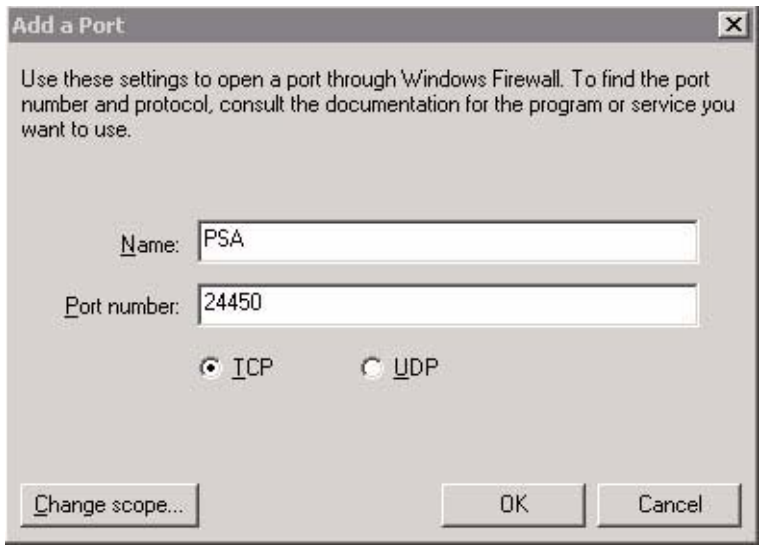


Abbildung 4.36 Dialogfenster [Add a Port]

4 Klicken Sie im Fenster [Windows Firewall] noch einmal auf die Schaltfläche [Add Port].
Das Dialogfenster [Add Port] wird geöffnet.

5 Geben Sie die Nummer des von SNMP benutzten Ports ein und klicken Sie auf [OK].

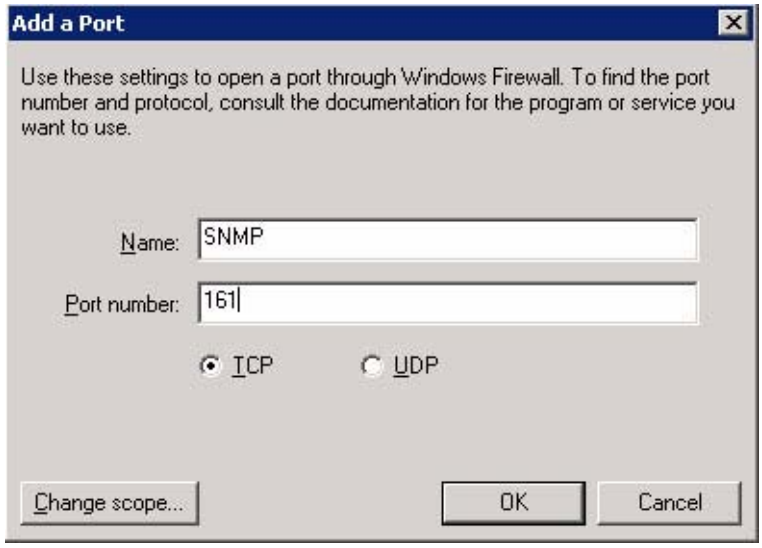


Abbildung 4.37 Dialogfenster [Add a Port]

6 Klicken Sie im Fenster [Windows Firewall] auf die Schaltfläche [OK], um die Einstellungen abzuschließen.

4.6.5 Watchdog-Überwachung nach Auftreten eines Stopp-Fehlers (eines schwerwiegenden Systemfehlers)

Tritt im System ein Stopp-Fehler (ein schwerwiegender Systemfehler) auf, passiert Folgendes:

PRIMEQUEST 520A*/520/420

- Unter „System Progress“ der entsprechenden Partition unter [Partition]-[Power Control] des MMB Web-UI wird „Panic“ ausgegeben.
- Ein Speicherabzug (Memory dump) des Systems wird erstellt.

Um in solchen Fällen zu verhindern, dass das System einfriert oder anderweitig nicht mehr antwortet, kann eine Überwachung mithilfe des Watchdog-Timers eingestellt werden.

Nach Ablauf der eingestellten Zeit führt MMB einen harten Reset aus, und das Betriebssystem wird neu gestartet.

Einstellungsablauf

1 Öffnen Sie folgende Datei:
[PSA-Installationsordner] \etc\opt\FJSVpsa\usr\pnwatchdog.conf
(Beispiel: C:\Program Files\fujitsu\FJSVpsa\etc\opt\FJSVpsa\usr \pnwatchdog.conf)

2 Geben Sie, wie unten dargestellt, einen Schlüsselwert ein. Standard ist 0.
Abschnitt: [WATCHDOG]
Schlüssel: [TIMER]
Wert einstellen (Einheit: Sekunden)0 (Watchdog-Timer wird nicht benutzt)
1 bis 6000 (Überwachungszeitraum des Watchdog-Timers)

Anm.: Wählen Sie beim Einstellen einen Wert, der 1,5 bis 2mal höher ist als die Zeit für einen Speicherabzug in der eingesetzten Systemumgebung. Ist der eingestellte Zeitraum kürzer als die benötigte Zeit für die Erstellung des Speicherabzugs, läuft die Zeit für den Watchdog-Timer ab, was zu einem harten Reset führt. Der Speicherabzug kann nicht mehr ordnungsgemäß abgeschlossen werden.

*: wird von Fujitsu Technology Solutions nicht unterstützt

4.6.6 PSA-Updates installieren

In diesem Abschnitt wird beschrieben, wie Sie ein PSA-Update installieren.

Anm.: Wenden Sie sich an Ihren Kundendienst-Techniker oder an das Support Center, um zu erfahren, wie Sie Fix-Programme erhalten.

Hinweis: Ist PEXU gemountet, benutzen Sie PSA ab Version 1.10.

(1) Kleinere Updates installieren

1 Speichern Sie das Fix-Programm (fjpsaxxxx.exe) im gewünschten Ordner.

2 Starten Sie das Fix-Programm. Der folgende Bildschirm zeigt an, dass die Installation vorbereitet wird:

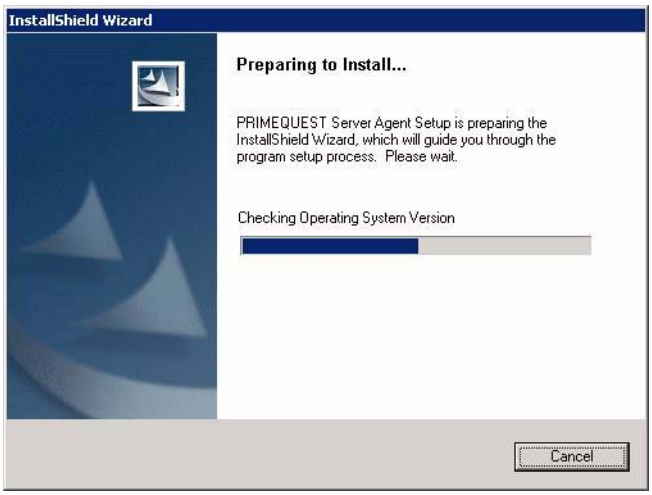

InstallShield Wizard
Preparing to Install...
PRIMEQUEST Server Agent Setup is preparing the InstallShield Wizard, which will guide you through the program setup process. Please wait.
Checking Operating System Version
Cancel

Abbildung 4.38 Installationsvorbereitung

3 Klicken Sie auf die Schaltfläche [Next], um die Installation auszuführen, wenn der folgende Bildschirm anzeigt, dass das System für die Installation bereit ist. Die Aktualisierung des Programms beginnt.

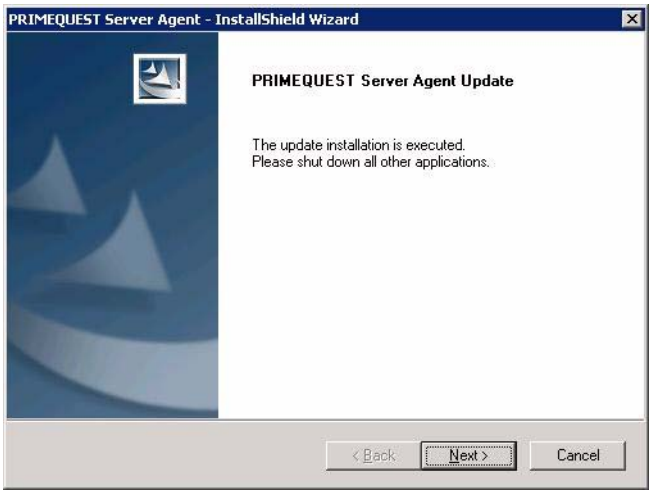

PRIMEQUEST Server Agent - InstallShield Wizard
PRIMEQUEST Server Agent Update
The update installation is executed.
Please shut down all other applications.
< Back
Next >
Cancel

Abbildung 4.39 Update-Installation

4 Klicken Sie auf die Schaltfläche [Finish], um den Vorgang abzuschließen.

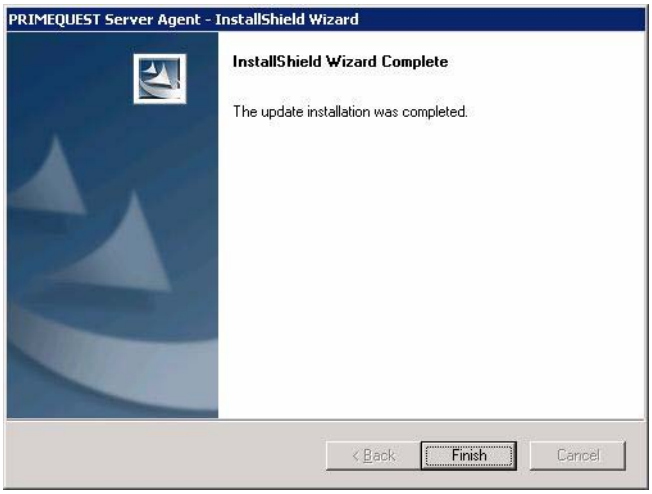


Abbildung 4.40 Update abgeschlossen

5 Wenn ein Neustart erforderlich ist, werden Sie in einem Dialogfeld gefragt, ob der Neustart durchgeführt werden soll. Überprüfen Sie, ob ein Neustart zum gegebenen Zeitpunkt problemlos durchgeführt werden kann und starten Sie das System dann neu, indem Sie auf die Schaltfläche [Finish] klicken.

(2) Umfangreichere Updates installieren

1 Speichern Sie das Fix-Programm (fjpsaxxxx.exe) im gewünschten Ordner.

2 Starten Sie das Fix-Programm. Der folgende Bildschirm zeigt an, dass die Installation vorbereitet wird:

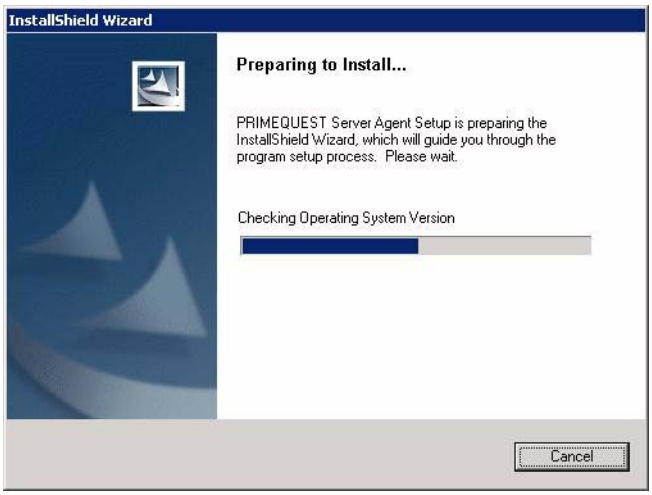

InstallShield Wizard
Preparing to Install...
PRIMEQUEST Server Agent Setup is preparing the InstallShield Wizard, which will guide you through the program setup process. Please wait.
Checking Operating System Version
Cancel

Abbildung 4.41 Installationsvorbereitung

3 Klicken Sie auf die Schaltfläche [OK], wenn das Bestätigungsfenster erscheint. Die Deinstallation wird daraufhin gestartet.

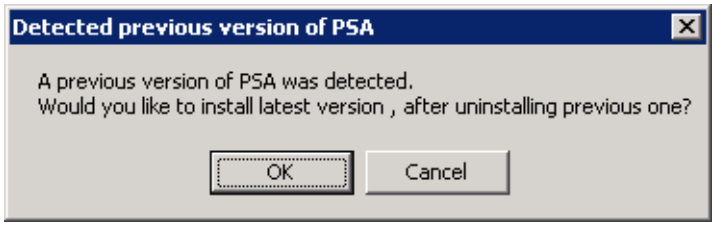

Detected previous version of PSA
A previous version of PSA was detected.
Would you like to install latest version , after uninstalling previous one?
OK
Cancel

Abbildung 4.42 [Detected previous version of PSA]

4 Wenn die Deinstallation abgeschlossen ist, wird die Installation der neuen Version gestartet.

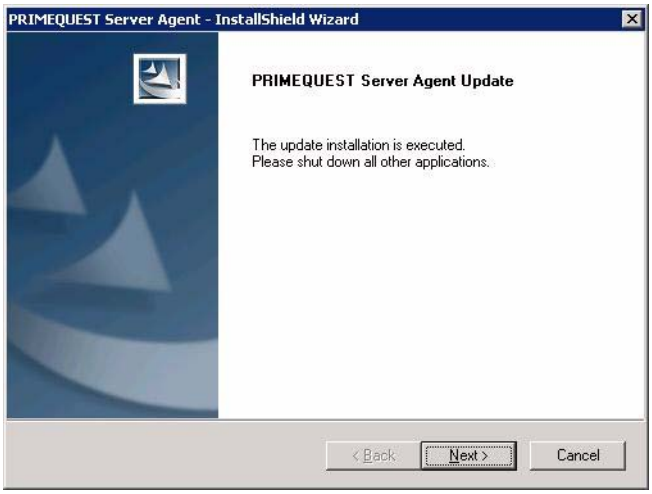

PRIMEQUEST Server Agent - InstallShield Wizard
PRIMEQUEST Server Agent Update
The update installation is executed.
Please shut down all other applications.
< Back
Next >
Cancel

Abbildung 4.43 Update-Installation

5 Geben Sie das Installationsziel an und klicken Sie dann auf die Schaltfläche [Next]. Die neue Version wird standardmäßig im Ordner „Program Files\Fujitsu“ installiert. Wenn Sie ein anderes Installationsziel bestimmen wollen, klicken Sie auf die Schaltfläche [Browse] und geben Sie das gewünschte Ziel an.

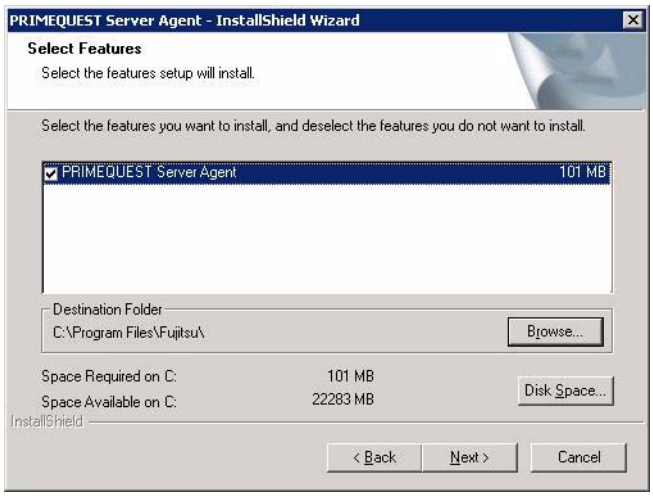


Abbildung 4.44 Fenster [Select Features]

6 Wenn die Installation abgeschlossen ist, wird das folgende Bestätigungsfenster angezeigt. Klicken Sie auf die Schaltfläche [Finish].

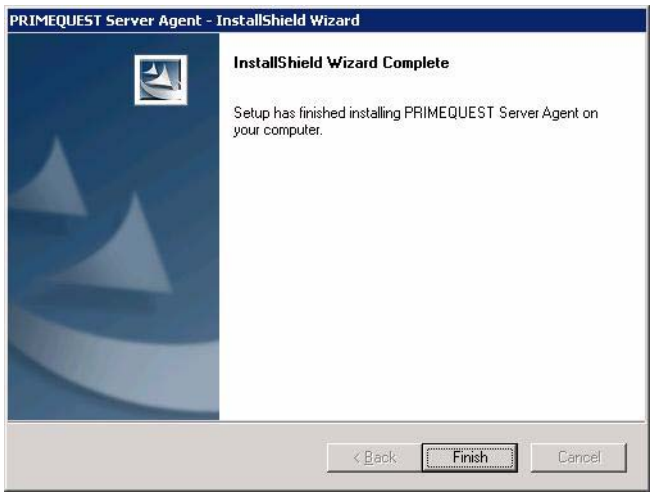


Abbildung 4.45 Installation abgeschlossen

7 Wenn ein Neustart erforderlich ist, werden Sie in einem Dialogfeld gefragt, ob der Neustart durchgeführt werden soll. Überprüfen Sie, ob ein Neustart zum gegebenen Zeitpunkt problemlos durchgeführt werden kann und starten Sie das System dann neu, indem Sie auf die Schaltfläche [Finish] klicken.

4.6.7 PSA deinstallieren

In diesem Abschnitt wird beschrieben, wie Sie PSA deinstallieren.

1 Wählen Sie [Control Panel] → [Add/Remove Programs] aus.

2 Wählen Sie unter [Currently Installed Programs] den Eintrag [PRIMEQUEST Server Agent] aus und klicken Sie auf die Schaltfläche [Change/Delete].

3 Sie werden aufgefordert, die Deinstallation zu bestätigen. Klicken Sie auf [OK], um die Deinstallation zu starten.

Abbildung 4.46 Bestätigungsfenster

4 Wenn die Deinstallation abgeschlossen ist, erscheint das folgende Bestätigungsfenster. Klicken Sie auf die Schaltfläche [Finish].

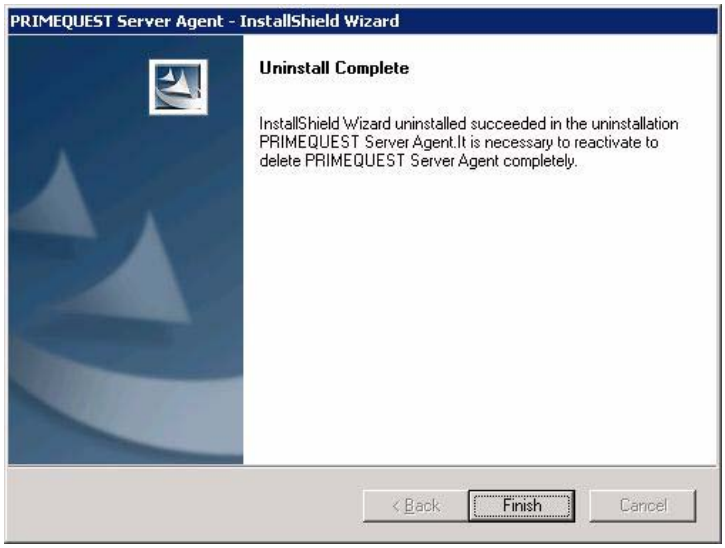

PRIMEQUEST Server Agent - InstallShield Wizard
Uninstall Complete
InstallShield Wizard uninstalled succeeded in the uninstallation PRIMEQUEST Server Agent.It is necessary to reactivate to delete PRIMEQUEST Server Agent completely.
< Back
Finish
Cancel

Abbildung 4.47 Deinstallation abgeschlossen

5 Wenn ein Neustart erforderlich ist, werden Sie in einem Dialogfeld gefragt, ob der Neustart durchgeführt werden soll. Überprüfen Sie, ob ein Neustart zum gegebenen Zeitpunkt problemlos durchgeführt werden kann und starten Sie das System dann neu, indem Sie auf die Schaltfläche [Finish] klicken.

4.7 PSA-Einstellungen

Einzelheiten zu den PSA-Einstellungen auf einem System mit Windows Server 2008 finden Sie im *PRIMEQUEST Windows Server 2008 User's Guide* (U41805-J-Z816-x-76/C122-E087EN).

4.8 PSA-Überwachung konfigurieren

Der PRIMEQUEST Server Agent (PSA) ist eine Applikation die auf dem Betriebssystem der PRIMEQUEST-Maschine läuft und den Zustand der Hardwarekomponenten überwacht und die Konfiguration aufrechterhält. In diesem Abschnitt werden die Einstellungen beschrieben, die während der Installation im PSA-Fenster vorgenommen werden müssen.

- S.M.A.R.T. einrichten (→ 4.8.1)
- Watchdog einrichten nach Auftreten eines Stopp-Fehlers (→ 4.8.2)

Abschnitt 4.13.1, „PSA-Konfigurationsdaten sichern“ beschreibt, wie Sie die gemachten Einstellungen sichern.

4.8.1 S.M.A.R.T. einrichten

Ziele für S.M.A.R.T. einstellen

S.M.A.R.T. steht für Self-Monitoring, Analysis and Reporting Technology, einer Funktion zur präventiven Laufwerksüberwachung. In diesem Abschnitt wird erläutert, wie Sie S.M.A.R.T. für Laufwerke aktivieren bzw. deaktivieren können, die diese Funktion unterstützen.
S.M.A.R.T. überwacht die folgenden Laufwerktypen:

- alle internen Laufwerke (die S.M.A.R.T. unterstützen)
- alle externe Laufwerke (außer RAID-Einheiten und jener Laufwerke, die S.M.A.R.T. nicht unterstützen)

Anm.: Zur Einrichtung oder Änderung von S.M.A.R.T. ist eine Schreibberechtigung erforderlich. Benutzer, die nur über Leseberechtigung verfügen, können S.M.A.R.T. nur anzeigen.

Überwachte Daten und Meldungen

- Überwachte Daten

  S.M.A.R.T. führt eine präventive Überwachung der unten aufgeführten Systemdaten durch und gibt bei Überschreitung der festgelegte Schwellenwerte eine Meldung aus. Die Schwellenwerte sind vom jeweiligen Laufwerktyp abhängig.

  - Temperatur
  - Lesefehler
  - Schreibfehler
  - Suchfehler
  - Hochfahrdauer
  - Anzahl verfügbarer Ersatzsektoren

  Nachdem S.M.A.R.T. konfiguriert wurde, werden die von S.M.A.R.T. gesammelten Daten zu jedem Laufwerk in regelmäßigen Abständen (zirka alle sechs Stunden) abgefragt, damit sich eventuell abzeichnende Fehler rechtzeitig erkannt und entsprechende Maßnahmen ergriffen werden können.

- Meldung bei Anzeichen für einen bevorstehenden Fehler
  - Die Fehler-LED des betreffenden Laufwerks leuchtet kontinuierlich vier Mal kurz hintereinander auf.
  - Die von S.M.A.R.T. gesammelten Daten werden in die SYSLOG-Datei ausgegeben und gemeldet (REMCS*/E-Mail).

*: wird von Fujitsu Technology Solutions nicht unterstützt

Vorgehensweise

1 Wählen Sie [Partition] → [Partition#x] → [PSA] → [Setup] → [S.M.A.R.T.]. Das Fenster [S.M.A.R.T.] wird angezeigt.

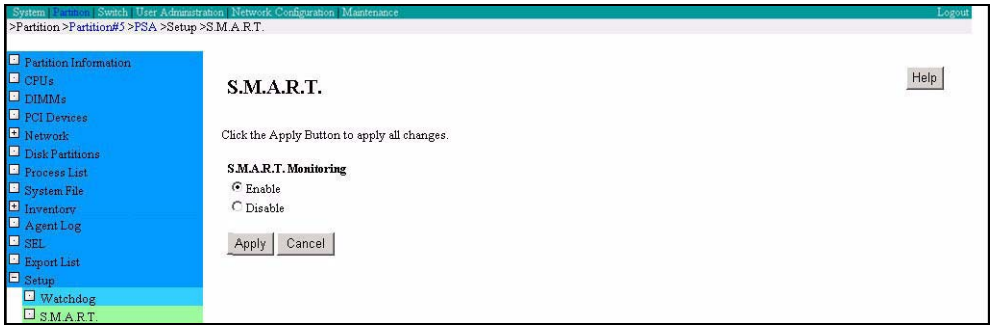


Abbildung 4.48 Das Fenster [S.M.A.R.T.]

2 Wählen Sie [Enable] oder [Disable] und klicken Sie dann auf [Apply], um Ihre Wahl zu bestätigen.

Position	Beschreibung
S.M.A.R.T. Monitoring	• [Enable]: aktiviert S.M.A.R.T. • [Disable]: deaktiviert S.M.A.R.T. Voreinstellung: [Enable]

4.8.2 Watchdog einrichten nach Auftreten eines Stopp-Fehlers

Überwachte Daten

Die Systemüberwachung mit Watchdog umfasst die Funktionen Software Watchdog und Boot Watchdog, die im Folgenden näher erläutert werden. Für eine Überwachung mit Watchdog müssen Timeout-Daten und Aktionen festgelegt werden (Aktionen stehen nur bei Software Watchdog zur Verfügung).

- Software Watchdog
  Die Funktion Software Watchdog veranlasst die MMB-Firmware, die Systembedingungen in regelmäßigen Abständen zu überprüfen. Ferner werden definierte Aktionen angestoßen, wenn das MMB nicht innerhalb eines festgelegten Zeitraums vom PSA angewiesen wird, den Watchdog-Timer zurückzusetzen.

- Boot Watchdog
  Die Funktion Boot Watchdog führt eine spezifische Aktion durch, wenn das Betriebssystem nicht innerhalb des festgelegten Zeitraums vollständig hochfährt. Die Boot Watchdog-Optionen werden, mit Ausnahme des Timeout-Wertes, im Fenster MMB ASR eingestellt. Dort kann Boot Watchdog in Notfällen auch deaktiviert werden.

Bevor Sie Watchdog einrichten

Messen Sie den TimeOut-Standardwert wie im Folgenden beschrieben, bevor Sie den TimeOut-Wert für den for Boot Watchdog einstellen.

Stellen Sie dann den Wert doppelt so hoch ein wie den gemessenen Wert, um einen ausreichenden Sicherheitsabstand zu gewährleisten.

Anm.: Diese Einstellung kann nur von einem Benutzer mit hinreichenden Rechten vorgenommen werden.

Hinweis: Wenn für Linux die Dump-Umgebung eingerichtet ist, stellen Sie auch die benötigte Dump-Speicherzeit ein, nachdem Sie die Dump-Umgebung eingerichtet haben.

1 Klicken Sie auf [Partition] → [Power Control].
Das [Power Control]-Fenster wird angezeigt.

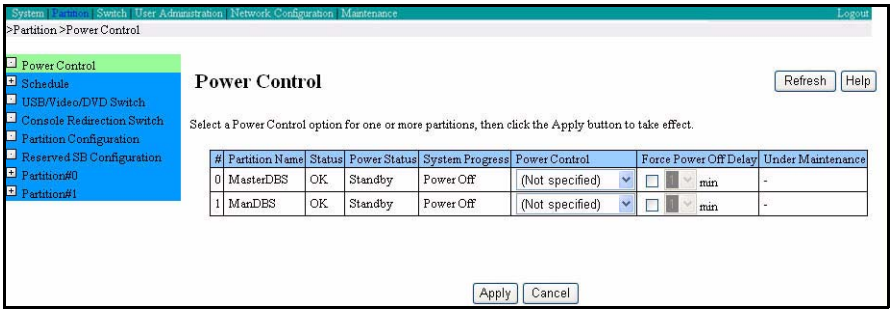

System | Partition | Switch | User Administration | Network Configuration | Maintenance
Logout
>Partition >Power Control
Power Control
Schedule
USB/Video/DVD Switch
Console Redirection Switch
Partition Configuration
Reserved SB Configuration
Partition#0
Partition#1
Power Control
Refresh
Help
Select a Power Control option for one or more partitions, then click the Apply button to take effect.
Partition Name Status Power Status System Progress Power Control Force Power Off Delay Under Maintenance
0 MasterDBS OK Standby Power Off (Not specified) min -
1 ManDBS OK Standby Power Off (Not specified) min -
Apply
Cancel

Abbildung 4.49 [Power Control]-Fenster

Linux

2 Stellen Sie sicher, dass das Feld [System Progress] der Partition, für die die Zeit gemessen werden soll, [OS Running] anzeigt.
Wählen Sie im [Power Control]-Fenster aus der Dropdown-Liste [INIT] aus und klicken Sie auf die Schaltfläche [Apply].

3 Nachdem die Dump-Information gesichert wurde, messen Sie die Zeit vom Start des Reboots der Partition bis im [System Progress]-Feld [OS Running] angezeigt wird.

Windows

2 Stellen Sie sicher, dass das Feld [System Progress] der Partition, für die die Zeit gemessen werden soll, [Power Off] anzeigt.
Wählen Sie im [Power Control]-Fenster aus der Dropdown-Liste [Power ON].

3 Messen Sie die Zeit vom Klicken auf [Apply] bis im [System Progress]-Feld [OS Running] angezeigt wird.

⚠ ACHTUNG

Fehlfunktion

Für das Ausführen der folgenden Operationen müssen Sie den Boot Watchdog auf [Disable] einstellen:

- Booten von CD-ROM
- Systemstart im Single User Mode
- Datensicherung und Datenwiederherstellung unter Verwendung des SystemcastWizard
  Falls diese Operationen ausgeführt werden, wenn der Boot Watchdog auf [Enable] eingestellt ist, wird der Wiederanlauf des Betriebssystems gemäß einer eingestellten Anzahl wiederholt, nachdem eine bestimmte Aktion ausgeführt wurde (Stop Reboot und Ausschalten, Stop Reboot oder Diagnostic Interrupt). Die Anzahl der Wiederanlaufsversuche und die Aktion werden im [ASR (Automatic Server Restart) Control]-Fenster des MMB eingestellt.
  Im [ASR (Automatic Server Restart) Control]-Fenster des MMB kann der Boot Watchdog auf [Disable] eingestellt werden, indem nach Markieren des [Cancel Boot Watchdog] [Apply] angeklickt wird.
  Einzelheiten zum [ASR (Automatic Server Restart) Control]-Fenster finden Sie in Abschnitt 5.3.11.3, „ASR (Automatic Server Restart) Control] window“ in PART III, „MMB“ des Handbuchs „*PRIMEQUEST 500A/500/400 Series Reference Manual: Basic Operation/GUI/Commands*“ (U41633-J-Z816-x-76/C122-E003EN).
- Wurde als Wert für die Anzahl der Wiederanlaufsversuche im [ASR (Automatic Server Restart) Control]-Fenster des MMB 0 eingestellt, wird die angegebene Aktion nicht einmal nach Ablauf der Zeit für einen Timeout ausgeführt. Geben Sie nicht 0 als Wert an, wenn Sie Watchdog-Überwachung einschalten.
  Näheres zum Fenster [ASR (Automatic Server Restart) Control] des MMB finden Sie in Abschnitt 5.3.11.3, „[ASR (Automatic Server Restart) Control] window“ in PART III „MMB“ des Handbuchs *PRIMEQUEST 500A/500/400 Series Reference Manual: Basic Operation/GUI/Commands* (U41633-J-Z816-x-76/C122-E003EN).

Vorgehensweise

1 Wählen Sie [Partition] → [Partition#x] → [PSA] → [Setup] → [Watchdog]. Das Fenster [Watchdog] wird angezeigt.

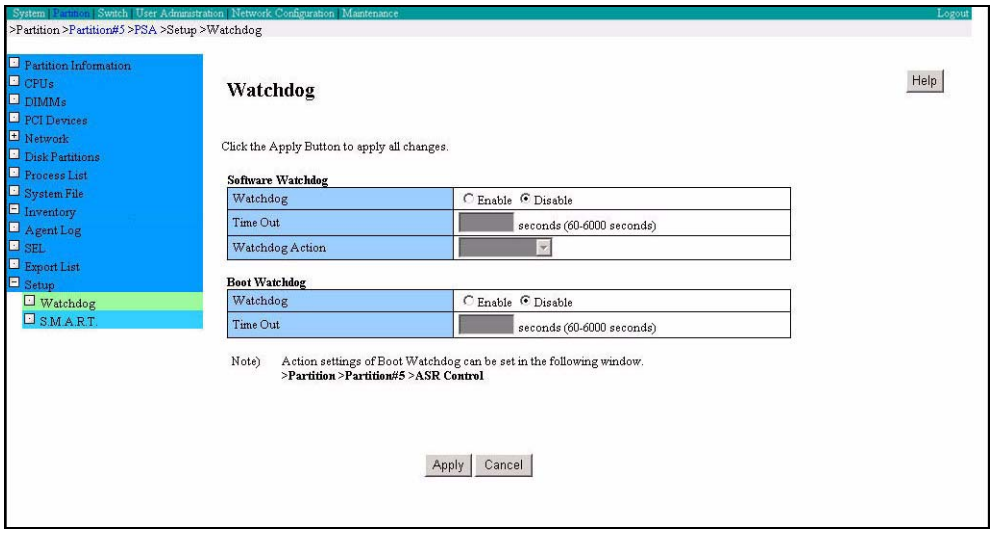


Abbildung 4.50 Das Fenster [Watchdog]

2 Geben Sie die erforderlichen Daten ein und klicken Sie auf [Apply], um sie zu übernehmen.

Tabelle 4.5 Ein- und Ausgabe von Daten im Fenster [Watchdog]

Feld	Beschreibung	
Software Watchdog	Watchdog	Sie können die Überwachung mit Software Watchdog aktivieren oder deaktivieren. [Disable]: Überwachung deaktivieren. [Enable]: Überwachung aktivieren. Voreinstellung: [Disable]
	TimeOut	Geben Sie einen Timeout-Wert in Sekunden an, wenn die Software Watchdog aktiviert ist: 60 - 6000 Sekunden. (Nur verfügbar, wenn [Watchdog] auf [Enable] gesetzt wurde.) Voreinstellung: 3600
	Watchdog Action	Wählen Sie aus der Dropdown-Liste die Maßnahme aus, die nach einem Timeout ergriffen werden soll, wenn eine Wiederherstellung fehlschlägt. • [No Action]: Keine Maßnahme, SEL-Output. • [Reset]: Partition neu starten. • [Power Off]: Partition ohne Shutdown des Betriebssystems ausschalten. • [Power Cycle]: Partition aus- und wieder einschalten • [INIT]: INIT-Verfahren für die Partition starten. (Nur verfügbar, wenn [Watchdog] auf [Enable] gesetzt wurde.) Voreinstellung: [No Action]

Tabelle 4.5 Ein- und Ausgabe von Daten im Fenster [Watchdog]

Feld	Beschreibung	
Boot Watchdog	Watchdog	Sie können die Überwachung mit Boot Watchdog aktivieren oder deaktivieren. [Disable]: Überwachung deaktivieren. [Enable]: Überwachung aktivieren. Hinweis:Stellen Sie Boot Watchdog auf [Disable] ein, wenn Sie eine der folgenden Operationen durchführen: • Boot CD-ROM • Systemstart im Single User Mode • Datensicherung und Datenwiederherstellung unter Verwendung des SystemcastWizard Voreinstellung: [Disable]
	TimeOut	Geben Sie einen Timeout-Wert in Sekunden an: 60 - 6000 Sekunden (Nur verfügbar, wenn Software Watchdog aktiviert wurde) Hinweis: Legen Sie den Wert aufgrund der Zeit fest, die die Partition vom Zeitpunkt des Einschaltens und wenn [System Progress] im Fenster [Power Control] des MMB auf [Boot] wechselt bis zu dem Zeitpunkt, wenn es auf [OS Running] wechselt, braucht. Es wird empfohlen, einen Wert etwas über dem Doppelten der o.g. Zeitdauer einzustellen, um fehlerhafte Meldungen zu vermeiden. Berücksichtigen Sie auch die Zeit, die nach einem Betriebssystem-Panic für das Speichern der Dump-Informationen benötigt wird. Diese Option ist nur verfügbar, wenn [Watchdog] auf [Enable] gesetzt wurde. Voreinstellung: 0. Eingabe erforderlich.

4.9 Dump-Umgebung einrichten (Linux: Red Hat)

Wenn unter Linux (Red Hat) die Dump-Funktion verwendet wird, muss vorab entsprechender Plattenspeicherplatz zugewiesen werden. Wie Sie den Plattenspeicherplatz zuweisen, ist im *PRIMEQUEST 580A/540A/580/540/480/440 System Design Guide* (U41630-J-Z816-x-76/C122-B001EN) oder *PRIMEQUEST 520A/520/420 System Design Guide* (U41643-J-Z816-x-76/C122-B009EN) beschrieben.

Wenn Linux (Red Hat) auf einer PRIMEQUEST betrieben wird, hängt der Einsatz der möglichen Dump-Funktion von der Linux Betriebssystem-Version ab. Im Folgenden wird kurz die Dump-Umgebung aller Linux Betriebssystem-Versionen beschrieben.

RHEL-AS4 (IPF)

Wenn RHEL-AS4 (IPF) auf einer PRIMEQUEST betrieben wird, kann die von Linux angebotene Dump-Funktion (diskdump) und die der PRIMEQUEST zugeordnete Dump-Funktion (sadump) verwendet werden.

Abbildung 4.51 gibt einen Überblick über die Dump-Umgebung.

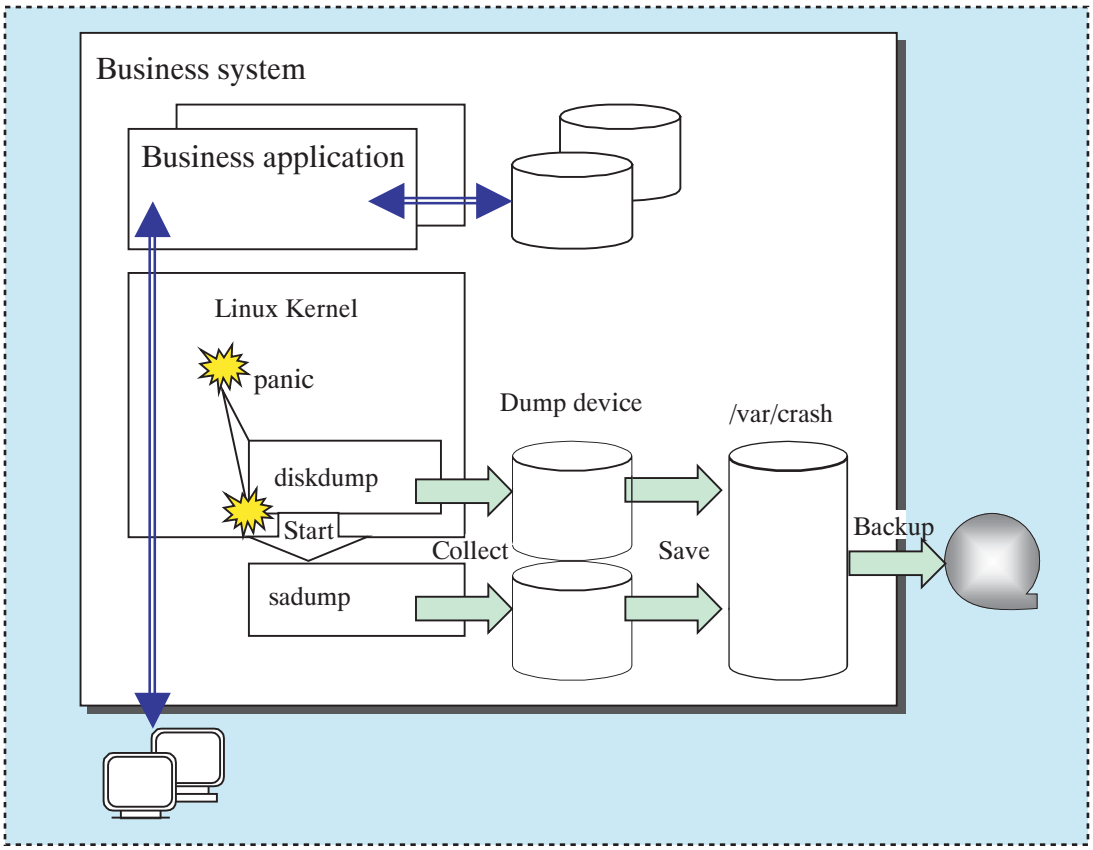


Abbildung 4.51 RHEL-AS4 (IPF) Dump-Umgebung

RHEL5 (IPF)

Wenn RHEL5 (IPF) mit PRIMEQUEST betrieben wird, kann die von Linux angebotene Dump-Funktion (kdump) und die der PRIMEQUEST zugeordnete Dump-Funktion (sadump) verwendet werden.

Abbildung 4.52 gibt einen Überblick über die Dump-Umgebung.

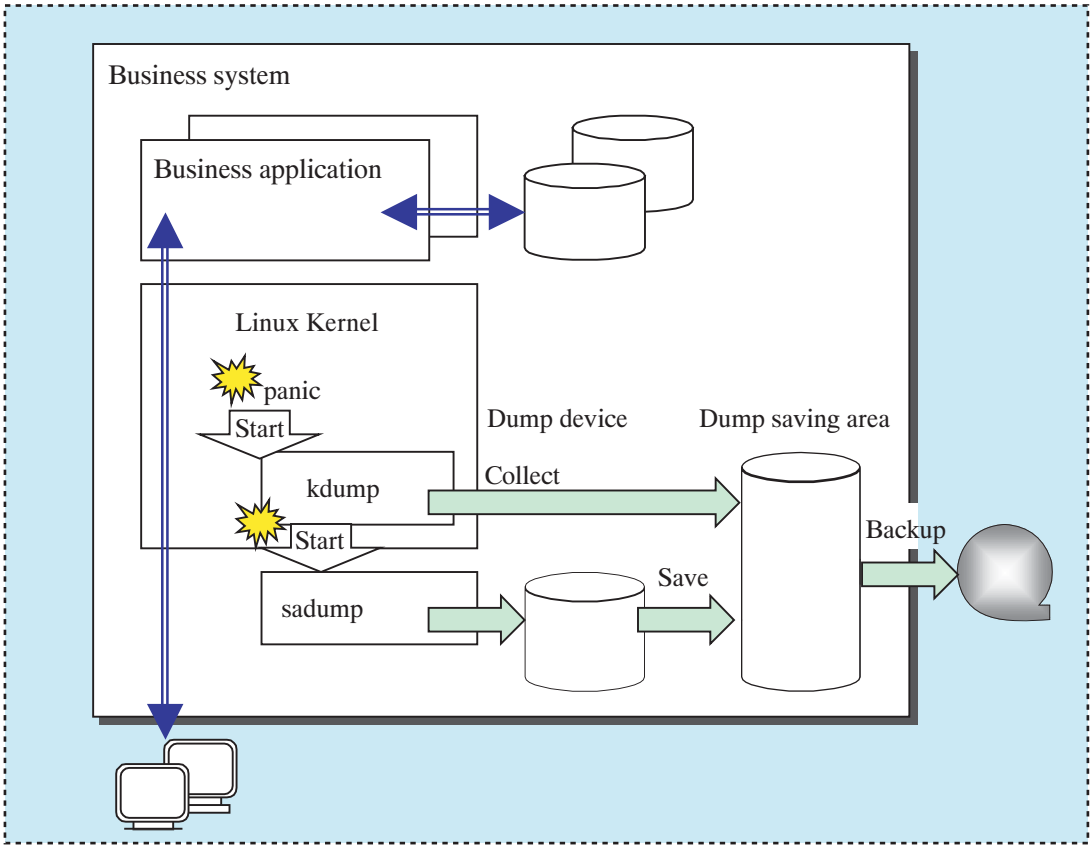


Abbildung 4.52 RHEL5 (IPF) Dump-Umgebung

In diesem Abschnitt wird beschrieben, wie Sie die Dump-Umgebung einrichten. Weitere Informationen zu Dump finden Sie im *PRIMEQUEST 500A/500/400 Series Reference Manual: Message/Logs* (U41634-J-Z816-x-76/C122-E004EN).

Wenn es zu einem Systemausfall kommt, sollte der Kundendienst von dem Vorfall unterrichtet werden. Dieser untersucht die Ursachen für den Vorfall auf der Grundlage der gesammelten Dump-Informationen. Damit diese Informationen gesammelt werden können, müssen zunächst die in den folgenden Abschnitten beschriebenen Schritte durchgeführt werden.

Das Sammeln der Speicher-Informationen funktioniert bei jedem Linux - Betriebssystem anders.

RHEL-AS4 (IPF)

Konfigurieren Sie die Dump-Umgebung nach folgender Prozedur:

- Dump-Umgebung einrichten
- Diskdump einrichten

RHEL5 (IPF)

- Dump-Umgebung einrichten
- kdump einrichten

In diesem Abschnitt werden die mit dem Dump verbundenen Aufgaben in der Reihenfolge beschrieben, in der sie auch ausgeführt werden sollen.

- Dump-Umgebung einrichten (→ 4.9.1)
- diskdump einrichten (→ 4.9.2)
- kdump einrichten (→ 4.9.3)

Für diese Einstellungen sind root-Berechtigungen erforderlich.

Hinweis: Einstellung der Umgebung aus einem X Window System oder aus einem Netzwerk wie telnet:
Richten Sie die Dump-Umgebung nach Möglichkeit in der Ebene 3 ein, ohne das X Window System zu benutzen. Wenn die Dump-Umgebung mit X Window System eingerichtet wird, werden einige Konsolenmeldungen nicht im X Window System angezeigt, so z.B. Meldungen bezüglich eines Speicherplatzmangels. Ferner werden einige Konsolenmeldungen nicht ausgegeben, wenn telnet oder ssh verwendet wird. Wenn Sie gezwungen sind, das X Window System zu benutzen, überprüfen Sie die Konsolenmeldungen mit dem Kommando dmesg oder /var/log/messages.

4.9.1 Dump-Umgebung einrichten

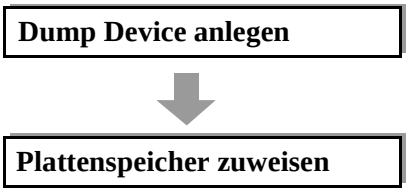
Die Arbeiten zur Nutzung der verschiedenen Dunp-Funktionen sind in den im Folgenden aufgeführten Abschnitten beschrieben. Führen Sie die erforderlichen Arbeiten mit root-Berechtigung aus.

- diskdump-Funktion von RHEL-AS4 (IPF):
  - 4.9.1.1, „Dump Device anlegen“
  - 4.9.1.2, „Dump-Speicherbereich zuweisen“
- kdump-Funktion von RHEL-AS4 (IPF):
  - 4.9.1.2, „Dump-Speicherbereich zuweisen“

Weitere Informationen zur Einschätzung des Plattenspeicherplatzes finden Sie im *PRIMEQUEST 580A/540A/580/540/480/440 System Design Guide* (U41630-J-Z816-x-76/C122-B001EN) oder *PRIMEQUEST 520A/520/420 System Design Guide* (U41643-J-Z816-x-76/C122-B009EN).

Anm.: Der Dump kann mit dem Installer auf der PRIMEQUEST Accessory CD-ROM automatisch eingerichtet werden.

Der im Folgenden wiedergegebene Arbeitsablauf erfordert root-Berechtigung.



In den folgenden Abschnitten werden die einzelnen Arbeitsschritte näher beschrieben.

4.9.1.1 Dump Device anlegen

Benutzen Sie das Kommando parted, um dem Dump Device einen Bereich zuzuweisen.

In dem hier verwendeten Beispiel wird das Dump-Gerät /dev/sdb1 angelegt.

```
# parted /dev/sdb
 (parted) mkpart primary 0 1000
 (parted) q
```

Legen Sie die Plattenpartition mit dem angegebenen Dateisystem an, um dem Dump Device bei der Installation des Linux-Betriebssystems eine Partition zuzuweisen. Wenn das System hochgefahren ist, hängen Sie die erstellte Partition aus und löschen Sie die entsprechenden Daten aus /etc/fstab.

Wenn Sie ein Dump Device erweitern wollen oder nach einem Ausfall neu anlegen wollen, ist eine Reinitialisierung erforderlich. Einzelheiten über die Initialisierung eines Dump Devices finden Sie in Abschnitt 4.9.2, „diskdump einrichten“.

Größe des Dump Devices

Weisen Sie dem Dump Device mit dem Kommando fdisk oder parted einen Bereich zu (Bereichtyp: Linux(83)).

Die Größe des einem Dump Device zugewiesenen Bereichs wird wie folgt errechnet:

```
Größe des Dump Devices = installierter Speicher* + 512 MB
```

* Wenn Extended Mirror Mode eingesetzt wird, entspricht die benutzbare Hauptspeichergröße der Hälfte des tatsächlich installierten Hauptspeichers. Der Speicher in der Formel oben entspricht dann dehalb nur die Hälfte des tatsächlich installierten Hauptspeichers.

Ein Dump Device kann nicht gemeinsam mit einem Dateisystem oder einer Swap-Partionen genutzt werden.

Gehen Sie wie folgt vor, um den benötigten Plattenspeicherplatz eines Dump Devices zu bestimmen.

```
# cat /proc/diskdump
# sample_rate: 8
# block_order: 2
# fallback_on_err: 1
# allow_risky_dumps: 1
# total_blocks: 262042

# getconf PAGESIZE
16384
```

Die Gesamtzahl der Blöcke wird in Speicherseiten wiedergegeben. In unserem Beispiel werden für das Dump Device „262.042 x 16.384“ Bytes benötigt.

Redundantes Dump Device

Legen Sie mindestens ein weiteres Dump Device an, um sicherzustellen, dass Sie auf die Dump-Daten zugreifen können, wenn das normalerweise benutzte Dump Device auf Grund eines Fehlers ausfällt. Jedes zusätzliche Dump Device sollte sich an einem anderen physikalischen Speicherort befinden.

Verwendbare Geräte

Die folgenden Geräte, die auf einem nicht duplizierten Laufwerk angelegt werden sollten, das nicht mit PRIMECLUSTER GDS verwaltet wird, können verwendet werden.

Tabelle 4.6 Als Dump Device einsetzbare Geräte

Gerätetyp	Treiber	Anmerkung
Internes Laufwerk	LSI Logic Fusion MPT (SCSI)	Unterstützt die interne SAS-Platte für die PRIMEQUEST 520A*/520/420
Externes Laufwerk	Emulex FC	
	LSI Logic Fusion MPT (SCSI)	Anschluss der SCSI-Platte über die SCSI-Karte in der PRIMEQUEST 520A*/520/420

*: wird von Fujitsu Technology Solutions nicht unterstützt

Es muss für jede Partition der PRIMEQUEST ein eigenes Dump Device eingerichtet werden. Dump Devices können nicht von mehreren Partitionen gemeinsam benutzt werden.

4.9.1.2 Dump-Speicherbereich zuweisen

Legen Sie einen Bereich zum Speichern des Dumps fest. Dieser Bereich heißt Dump-Speicherbereich. Weisen sie jeder Partition einen solchen Bereich zu. Beachten Sie dabei, dass ein Bereich nicht von mehreren Partitionen genutzt werden kann. Der Bereich zum Speichern des Dumps variiert von einem Linux-Betriebssystem zum andern.

Überprüfen Sie den Dump-Speicherbereich.

- RHEL-AS4 (IPF)
  Der Dump-Speicherbereich ist /var/crash.
  Führen sie folgende Operation durch, um zu überprüfen, ob das Verzeichnis existiert.

```
# ls -l /var/crash
```

- RHEL5 (IPF)
  Reservieren Sie eine geeignete Partition (Beispiel: /dev/sdb2) als Dump-Speicherbereich und formatieren Sie ihn als Dateisystem (Beispiel: ext3). Überprüfen Sie mit Hilfe der folgenden Operation, ob dieses Verzeichnis korrekt erstellt wurde.

```
# mount /dev/sdb2 /var/crash
# ls -l /var/crash
```

  Um den Verlust von Daten während der Operation zu vermeiden, stellen Sie sicher, dass der Dump-Speicherbereich nicht gemountet wird.

Bei Linux (Red Hat) richten Sie folgenden freien Bereich als Dump-Speicherbereich ein.

```
Größe des Dump-Speicherbereichs
= (installierter Speicher* + 1 GB) x Anzahl der temporär gespeicherten Dump-Dateien
```

* Wenn Extended Mirror Mode eingesetzt wird, entspricht die benutzbare Hauptspeichergröße der Hälfte des tatsächlich installierten Hauptspeichers. Der Speicher in der Formel oben entspricht dann dehalb nur die Hälfte des tatsächlich installierten Hauptspeichers.

Wieviel Speicherplatz Sie in etwa für Dumps benötigen, können Sie anhand der maximalen Anzahl Dump-Dateien ermitteln, die temporär auf dem System gespeichert werden. Wenn eine Dump-Datei bei Auftreten eines Fehlers direkt nach dem Neustart auf ein Speichermedium, beispielsweise auf ein Band, ausgelagert werden kann, gehen Sie von zwei temporären Dump-Dateien (dsikdump/kdump und sadump können gleichzeitig korrigiert werden) aus. Wenn der zugewiesene Speicherplatz knapp wird, können die Dump-Dateien nicht korrelt gespeichert werden. Verwalten Sie den freien Plattenspeicherplatz sorgfältig und lagern Sie erstellte Dump-Dateien so schnell wie möglich auf ein externes Speichermedium aus anstatt sie auf der Platte zu belassen.

Hinweis: Wenn das Kommando parted benutzt wird, um die Größe des Dump-Speicherbereichs innerhalb von RHEL5 zu überprüfen, geben Sie „unit MiB“ ein, um die Ausgabeeinheit zu ändern. Das Kommando parted gibt die Größe der gesamten Platten-Partition einschließlich des Verwaltungsbereichs aus, der vom Dateisystem ext3 belegt wird. Teilen Sie deshalb den ausgegebenen Wert für die Größe durch 1,1, um die Größe des nötigen Dump-Speicherbereichs zu erhalten, in dem eine ext3-Datei erstellt werden kann.

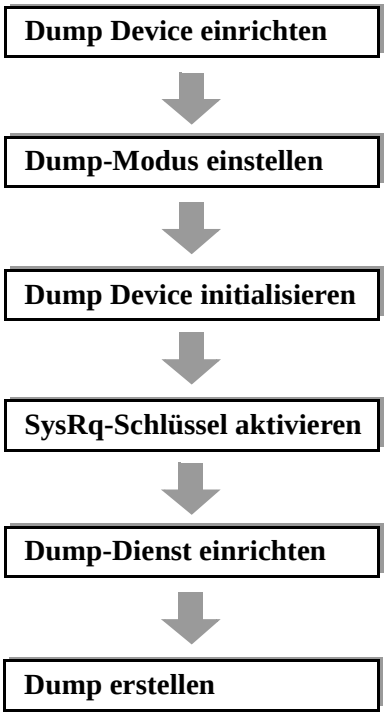
Wenn ein Dump ordnungsgemäß gespeichert wird, wird eine Datei namens vmcore erstellt. Wenn der Speicherplatz unzureichend ist, wird ein unvollständiger Dump unter dem Namen vmcore_incomplete gespeichert. Wenn unter RHEL-AS4 (IPF) der Speicherplatz unzureichend ist, wird ein Skript mit dem Namen diskdump-nospace, das der Benutzer editieren kann, gestartet, bevor ein Fehler auftritt. Bearbeiten Sie das Skript so, dass ausreichend Speicherplatz vorhanden ist. Legen Sie das Skript unter /var/crash/scripts an. Falls der Dump-Speicherbereich nicht existiert, erstellen Sie das benötigte Verzeichnis. Wenn das Verzeichnis wegen einer Erweiterung oder eines Fehlers des Dump-Speicherbereichs neu angelegt werden muss, erstellen Sie es in der üblichen Weise.

Wenn Sie diskdump anwenden, ist der Dump-Speicherbereich auf /var/crash festgelegt. Die Dump-Speicherbereiche für kdump und sadump sind jedoch nicht festgelegt. Erstellungsmethoden dafür finden Sie unter Abschnitt 4.9.3.3, „Dump-Umgebung einrichten“.

4.9.2 diskdump einrichten

In diesem Abschnitt werden die ersten Einstellungen erläutert, die zur Nutzung der Dump-Funktion erforderlich und im Lieferunfang enthalten sind.

Da diskdump Bestandteil des Lieferumfangs von RHEL-AS4 (IPF) ist, muss es nicht separat installiert werden. Führen Sie nach der Installation von RHEL-AS4 (IPF) lediglich unter root-Berechtigung die nachfolgend beschriebenen Schritte aus.



Im Folgenden werden die einzelnen Schritte genauer beschrieben.

(1) Dump Device einrichten

Fügen Sie der Definition von diskdump (/etc/sysconfig/diskdump) mit einem Texteditor, beispielsweise mit vi, folgende Definition hinzu:

```
DEVICE=geräte-name (Beispiel:  DEVICE=/dev/sde1)
```

Hinweis: Geben Sie den Namen eines geeigneten Geräts ein.

Anm.: Benutzen Sie als Trennzeichen zwischen den einzelnen Gerätenamen einen Doppelpunkt (:), wenn Sie mehrere Dump Devices erstellen, von denen mindestens eines redundant sein sollte.

(2) Dump-Modus einstellen

Fügen Sie in /etc/modporbe.conf mit einem Texteditor, beispielsweise mit vi, folgende Zeile ein, um durch Nutzung einer partiellen Dump-Funktion Speicherplatz zu sparen:

```
options diskdump dump_level=n
```

Dabei ist n der zur Anwendung kommende Dump-Modus:

0: Dump des gesamten Speicherinhalts.

19: Verwendung der partiellen Dump-Funktion.

Verwenden Sie die partielle Dump-Funktion, um die Belastung durch ein Dump zu verringern, wenn ein umfangreicher Speicher installiert ist. Wenn dieser Dump-Modus nicht eingestellt wird, wird der gesamte Speicherinhalt in die Dump-Datei gestellt.

Fügen Sie in /etc/modporbe.conf mit einem Texteditor, beispielsweise mit vi, folgende Zeile ein, um mit der Kompressionsfunktion den für ein Dump benötigten Speicherplatz zu reduzieren:

```
options diskdump compress=1
```

Verwenden sie das Kommando file, wie Sie es im Folgenden sehen, um die Kompression des Dump-Bereichs zu überprüfen.

- Wenn der Dump-Bereich nicht komprimiert ist
  Wie das folgende Beispiel zeigt, wird eine Datei im ELF-Format ausgegeben.

```
# file vmcore
vmcore: ELF 64-bit LSB core file IA-64, version 1 (SYSV), SVR4-
style, from 'vmlinux'
```

- Wenn der Dump-Bereich komprimiert ist

```
# file vmcore
vmcore: data
```

Wenn der Typ der Dump-Datei zurückgesetzt wurde während der Service diskdump aktiv war, muss das System reaktiviert werden.

(3) Dump Device initialisieren

Gehen Sie wie folgt vor, um ein Dump Device zu initialisieren. Überprüfen Sie das Ergebnis anhand des Rückgabewerts. Bei einem Rückgabewert 0 wurde die Initialisierung erfolgreich abgeschlossen.

```
# service diskdump initialformat
```

Hinweis: Der Speicherbereich des Dump Device darf nicht von einem Dateisystem oder einem anderen Gerät mit benutzt werden. Stellen Sie sicher, dass im Speicherbereich des Dump Device keine Daten gespeichert sind, da diese vom Kommando initialformat überschrieben werden.

(4) SysRq-Schlüssel aktivieren

Gehen Sie wie folgt vor, um den [SysRq]-Schlüssel zu aktivieren:

- Mit System Parameter Check Tool

Geben Sie das folgende Kommando ein:

```
# /usr/sbin/fjprmset -f -S -a kernel.sysrq=1
```

Eine „1“ bedeutet, die Einstellungen wurden bestätigt.

```
# cat /proc/sys/kernel/sysrq
```

Näheres über das System Parameter Check Tool finden Sie in Anhang A.5, „System Parameter Check Tool“.

- Ohne System Parameter Check Tool

Ändern Sie den Wert für kernel/sysrq in der Datei /etc/sysctl.conf, um die Einstellungen zu überprüfen.

```
# vi /etc/sysctl.conf
```

Zeile ändern bzw. hinzufügen:

```
kernel.sysrq = 1
```

```
# sysctl -p
```

Geben Sie das folgende Kommando ein. Wird eine „1“ angezeigt, können Sie davon ausgehen, dass die Einstellung wiedergegeben wird.

```
# cat /proc/sys/kernel/sysrq
```

(5) Dump Service einstellen

Führen Sie das folgende Kommando aus, um einen Dump Service so einzustellen, dass er mit einem Boot beginnt.

```
# chkconfig diskdump on
```

Mit dem folgenden Kommando kann der Benutzer überprüfen, ob die Einstellung ordnungsgemäß gemacht werden kann.

```
# chkconfig -list diskdump
```

Folgende Einstellungen werden angezeigt:

```
diskdump  0:ff  1:off  2:on  3:on  4:on  5:on  6:off
```

(6) Dump-Erstellung überprüfen

1 Dump Service starten

Starten Sie den Dump Service mit folgendem Kommando:

```
# service diskdump start
```

Anm.: Wenn das Dump-Gerät kleiner als der installierte Speicher ist, wird die folgende Meldung ausgegeben. Ändern Sie in dem Fall die Größe des Dump Devices.

```
disk_dump: xx: is too small to save whole system memory
(xx: Geräte-Name)
```

Folgende Meldungen werden ausgegeben, wenn der Dienst gestartet wird. Ignorieren Sie diese Meldungen.

```
PRESERVEDUMP not enabled
SKIPSAVECORE not enabled
SALVAGEMESSAGE enabled
```

2 Dump-Erstellung überprüfen

Wenn es zu einem Systemabsturz kommt, kann der Dump nicht erstellt werden, wenn der Speicherplatz nicht ausreicht. Überprüfen Sie daher, ob der Crash Dump erstellt wurde.

Hinweis: Wenn die Erstellung des Crash Dump erzwungen wird, wird ein Systemabsturz erzwungen. Beenden Sie also vorher alle wichtigen Anwendungen. Dateisysteme, die nicht benötigt werden, sollten ebenfalls vorher ausgehängt werden.

1 Dump manuell erstellen.
Wählen Sie im Menü [Power Control] der MMB Web-UI den Eintrag [Partition] aus, wählen Sie [INIT] aus, und klicken Sie auf [Apply].

- Überprüfen Sie, ob die Dump-Verarbeitung abgeschlossen ist.
  Überprüfen Sie, ob die folgende Meldung auf der Konsole angezeigt wird:

```
Rebooting in nn seconds.
(nn ist die Zeit in Sekunden bis zum Neustart.)
```

oder

```
halt
```

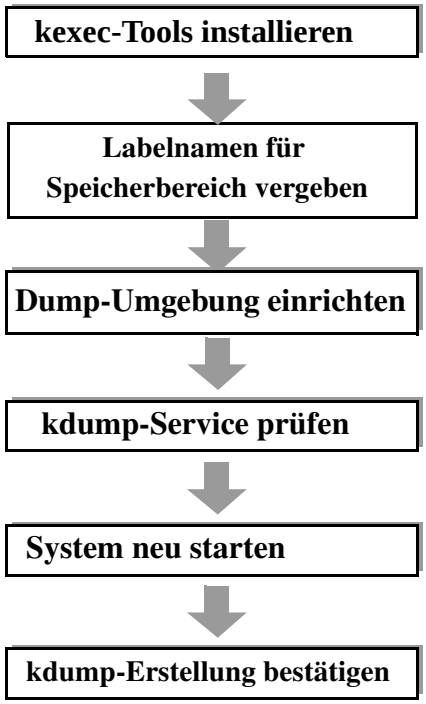
2 Starten Sie das System neu.
Wenn ein automatischer Neustart festgelegt wurde, warten Sie, bis das System neu startet. Wenn ein Systemstop festgelegt wurde, führen Sie einen Neustart durch. Wählen Sie dazu in der MMB Web-UI [Partition] → [Power Control] aus, wählen Sie den Status [Reset] und klicken Sie auf [Apply].

3 Überprüfen Sie, ob der Dump erstellt wurde.
Gehen Sie dafür wie folgt vor:
- Überprüfen Sie, ob ein Verzeichnis /var/crash/127.0.0.1-[Datum und Uhrzeit] erstellt wurde.
- Um zu überprüfen, ob ein Dump abgelegt wurde, schauen Sie nach, ob eine Datei vmcore im oben genannten Verzeichnis angelegt wurde.

4 Löschen Sie das Test-Dump mit dem Kommando rm wieder aus dem obigen Verzeichnis.

4.9.3 kdump einrichten

Dieser Abschnitt erläutert die Ersteinrichtung der Dump-Funktion, die im Lieferumfang enthalten ist. Obwohl kdump Bestandteil von RHEL5 (IPF) ist, können die erforderlichen Pakete abhängig von den Einstellungen in RHEL5 (IPF) evtl. nicht angewendet werden. Dieser Abschnitt beschreibt die Ersteinstellungen für kdump, sowie die Anwendung dieser Pakete. Die Ersteinstellung für kdump läuft folgendermaßen ab:



4.9.3.1 kexec-Tools installieren

Es ist möglich, dass das für kdump erforderliche Paket kexec-tools abhängig von der Installation von RHEL5 (IPF) nicht automatisch installiert ist. Installieren Sie es deswegen bei Bedarf manuell wie folgt:

```
# rpm -q kexec-tools
# rpm -ivh kexec-tools-<version/level to be installed>.el5.ia64.rpm
```

Eventuell müssen kernel-debuginfo und kernel-debuginfo-common auch installiert werden. Installieren Sie sie bei Bedarf wie folgt:

```
# rpm -q kernel-debuginfo-common
# rpm -q kernel-debuginfo
# rpm -ivh kernel-debuginfo-common-<version/level to be installed>
.el5.ia64.rpm
# rpm -ivh kernel-debuginfo-<version/level to be installed>.el5.ia64.rpm
```

4.9.3.2 Vergeben eines Labels für den Dump-Speicherbereich

Verwenden Sie das Kommando e2label, um ein Label für den Bereich zu vergeben, in den ein Dump gesichert werden soll.

```
# e2label /dev/sdb2 /dump                    Set
# e2label /dev/sdb2                          Verify
/dump
```

4.9.3.3 Dump-Umgebung einrichten

Mit /etc/kdump.conf geben Sie den Bereich an, in den der Dump gesichert werden soll. Machen Sie auch die Einstellungen für die Dump-Funktion und anderes. Die Einstellungsprozedur ist anhand eines Definitionsbeispiels weiter unten erklärt. Codieren Sie die Teile, die nicht erklärt sind, so, wie es im Definitionsbeispiel gezeigt wird.

```
ext3 LABEL=/dump
           ~~~~~(1)
path /
core_collector makedumpfile
default reboot
~~~~~~~~~~~~~~(2)
```

1 Setzen Sie /dump und das Label für den Bereich, in den der Dump gesichert werden soll, und definieren Sie das Label als Dump-Speicherbereich.

2 Geben Sie reboot als auszuführende Operation nach der Dump-Erstellung an. Wurde sadump angewendet, folgt die sadump-Definition nach der kdump-Erstellung, und deshalb werden die hier gesetzten Werte ignoriert.

```
core_collector makedumpfile -c -d 3
                            ~(3)~~~~(4)
```

3 Geben Sie dies an, wenn Sie die komprimierte Dump-Funktion nutzen wollen. Lassen Sie es weg, wenn die Funktion nicht benutzt wird. Die komprimierte Dump-Funktion mag den Dump-Speicherbereich reduzieren, braucht dafür aber eventuell länger für die Dump-Erstellung. Führen Sie eine ausreichende Leistungsüberprüfung durch, bevor Sie die komprimierte Dump-Funktion einschalten.

4 Geben Sie dies an, wenn Sie die partielle Dump-Funktion nutzen wollen. Lassen Sie es weg, wenn die Funktion nicht benutzt wird. Fügen Sie außerdem folgende Definition zu KDUMP_COMMANDLINE_APPEND von /etc/sysconfig/kdump hinzu.

```
swiotlb=128
```

Wenn /etc/kdump.conf wieder gesetzt wird, muss der Dienst sadump oder das System neu gestartet werden.

4.9.3.4 kdump-Dienst einrichten

Geben Sie Folgendes ein, damit der kdump-Dienst beim Booten des Systems automatisch startet.

```
# chkconfig kdump on
```

Geben Sie Folgendes ein, um zu überprüfen, ob der Dump-Service korrekt eingerichtet ist.

```
# chkconfig -- list kdump
```

Die Einstellungen werden folgendermaßen ausgegeben:

```
kdump  0:off 1:off 2:on 3:on 4:on 5:on 6:off
```

4.9.3.5 Kernel-Parameter setzen

Geben Sie mit Hilfe des Kernel-Parameters append Folgendes in /boot/efi/efi/redhat/elilo.conf ein.

```
append=" ··· crashkernel=512M@256M"
```

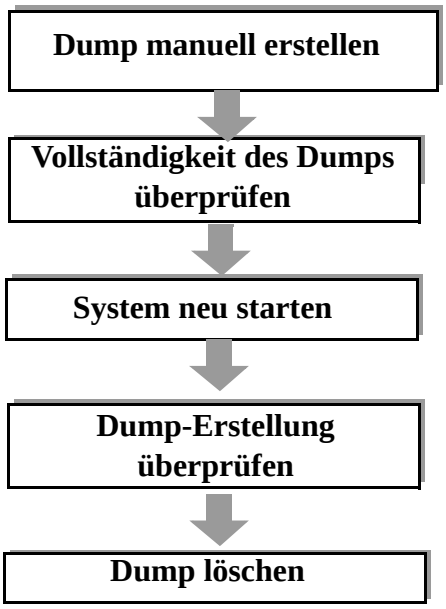
4.9.3.6 System neu starten

Geben Sie Folgendes ein, um das System neu zu starten.

```
# reboot
```

4.9.3.7 kdump-Erstellung überprüfen

Stürzt das System wirklich ab, kann es passieren, dass der Dump aus Platzmangel nicht erstellt wird. Um dies zu verhindern, überprüfen Sie vorher mit folgender Prozedur, ob der Crash Dump wirklich erstellt wird:



Hinweis: Wenn die Erstellung des Crash Dump erzwungen wird, wird ein Systemabsturz erzwungen. Beenden Sie also vorher alle wichtigen Anwendungen. Dateisysteme, die nicht benötigt werden, sollten ebenfalls vorher ausgehängt werden.

(1) Dump manuell erstellen

Wählen Sie im Menü [Power Control] der MMB Web-UI den Eintrag [Partition] aus, wählen Sie [INIT] aus, und klicken Sie auf [Apply], um die Dump-Erstellung zu starten.

(2) Überprüfen, ob die Dump-Erstellung abgeschlossen ist

Mit folgender Meldung auf der Konsole stellen Sie sicher, dass die Dump-Erstellung abgeschlossen ist:

```
makedumpfile Completed.
```

Hinweis: Wurde der Dump erfolgreich erstellt, wird wahrscheinlich die im folgenden Beispiel gezeigte Meldung ausgegeben. (Beachten Sie, dass der wirkliche Name der Dump-Datei nicht vmcore-incomplete, sondern vmcore ist.)

```
The dumpfile is saved to /mnt/127.0.0.1-2007-02-14-15:20:37/vmcore-
incomplete.
```

(3) System neu starten

Das System wird automatisch neu gestartet. Warten Sie, bis der Neustart abgeschlossen ist.

(4) Dump-Erstellung überprüfen

Überprüfen Sie folgendermaßen, ob der Dump erstellt wurde:

- Überprüfen Sie, ob ein Verzeichnis „127.0.0.1-[date and time]“ im Bereich für das Speichern des Dumps erstellt wurde.

  Hinweis: Ist „UTC = false“ in /etc/sysconfig/clock eingestellt, ist das ausgegebene Datum/Zeit 9 Stunden später als Datum/Zeit der Dump-Erstellung. Missverstehen Sie es nicht als Datum/Zeit der Dump-Erstellung.

- Überprüfen Sie, ob der Dump erstellt wurde oder die Größe von vmcore im oben angegebenen Verzeichnis mehr oder weniger der geschätzten Größe der Dump-Datei entspricht.

Da der Dump-Speicherbereich nicht mit dem Betriebssystem-Kernel gemountet wird, überprüfen Sie die Dump-Erstellung wie oben beschrieben nach dem Mounten des Dump-Speicherbereichs.

(5) Dump löschen

Mit dem Kommando rm löschen Sie den erstellten Test-Dump. Zum Abschluss hängen Sie den Dump-Speicherbereich aus.

4.10 Dump-Umgebung einrichten (Windows Server 2003)

Windows Server 2003 erlaubt Ihnen, Dumps mit Standardfunktionen es Betriebssystems zu erstellen. Bevor Sie ein Dump erstellen können, müssen Sie einen Systembereich zuweisen. Näheres zu diesem Verfahren ist im *PRIMEQUEST 580A/540A/580/540/480/440 System Design Guide* (U41630-J-Z816-x-76/C122-B001EN) oder *PRIMEQUEST 520A/520/420 System Design Guide* (U41643-J-Z816-x-76/C122-B009EN) enthalten.

In diesem Abschnitt wird beschrieben, wie Sie eine Umgebung einrichten können, in der mit Windows Server 2003 ein Dump erstellt wird. Weitere Informationen hierzu finden Sie auch im Kapitel 1 „System Maintenance“ des *PRIMEQUEST 500A/500/400 Series Reference Manual: Tools/Operation Information* (U41757-J-Z816-x-76/(C122-E074EN)).

Um eine Wiederherstellung des Systems nach einem Fehler zu ermöglichen, müssen zunächst die in den folgenden Abschnitten beschrieben Einstellungen vorgenommen werden:

- Memory Dump- und Paging-Datei einrichten (→ 4.10.1)
- Präventive Fehlerbehebung mit [DSNAP] (→ 4.10.2)

4.10.1 Memory Dump- und Paging-Datei einrichten

In diesem Abschnitt wird beschrieben, wie Sie eine Dump- und eine Paging-Datei einrichten.

Eine Memory Dump-Datei (Speicherabzugsdatei) enthält Debug-Informationen, wenn ein fataler Systemfehlers (STOP) im System auftritt. Nachdem das Betriebssystem und die für den Betrieb erforderlichen Anwendungen installiert sind, nehmen Sie die für den Meomry Dump nötigen Einstellungen vor.

4.10.1.1 Art der Informationen, die aus einem Memory Dump gewonnen werden können

Folgende drei Arten von Memory Dumps können auf einem PRIMEQUEST-System eingerichtet werden. Sie unterscheiden sich im Umfang der gespeicherten Informationen.

Stellen Sie sicher, dass die Festplatte genügend freien Speicherplatz hat, bevor Sie einen Memory Dump starten.

- Vollständiger Memory Dump
  Speichert den kompletten Inhalt des physikalischen Speichers, wenn das System anhält. Der Boot-Datenträger muss ungefähr 1 Megabyte mehr freien Speicherplatz haben als der physikalische Speicher. Es kann nur ein Dump gespeichert werden. Befindet sich bereits ein Dump im festgelegten Speicherplatz, wird die Dump-Datei überschrieben.
- Kernel-Dump (empfohlen)
  Es wird nur der Inhalt des Kernel-Dumps aufgezeichnet. Der Boot-Datenträger muss zwischen 50 und mehreren hundert Megabyte Platz haben (bis zur physikalischen Speichergröße plus 128 Megabyte). Die Größe hängt vom Betriebszustand ab. Der Boot-Datenträger nur einen Dump speichern. Befindet sich bereits ein Dump im festgelegten Speicherplatz, wird die Dump-Datei überschrieben.
- Kleiner Dump
  Es wird die Mindestmenge der für die Identifizierung eines Problems erforderlichen Daten aufgezeichnet. Dieser Memory Dump erfordert 64 oder 128 Kilobyte freien Speicherplatz. Bei Wahl dieser Option wird jedes Mal eine Datei erzeugt, wenn das System umerwartet stoppt.

Tabelle 4.7 Art und Größe des Dumps

Art des Memory-Dump	Memory Dump-Datei	
Vollständiger Memory Dump	Physikalische Speichergröße + 1 MB	Overwrite (*2)
Kernel-Dump	Hängt von der Größe des Speichers ab, den das Betriebssystem im laufenden Betrieb benutzt (normalerweise 50 bis zu einigen hundert MB). Maximal: installierter physikalischer Speicher + 128 MB (*1)	Overwrite (*2)
Kleiner Dump	64 KB bzw. 128 KB	Neue Datei wird erzeugt

*1 Hier ist die maximal mögliche Größe angegeben. Die tatsächliche Größe hängt jedoch von der Größe des installierten Speichers ab.

*2 Standardmäßig wird eine bestehende Datei überschrieben. Die Standardeinstellung kann dahingehend geändert werden, dass eine bestehende Datei nicht überschrieben wird. Beachten sie jedoch, dass keine neue Datei angelegt wird, anders als beim „kleinen Dump“.

Hinweise: Wählen sie den für den Systembetrieb passenden Modus unter folgenden Gesichtspunkten aus:

- Wird der PRIMEQUEST Software Installer angewendet, wird automatisch der Modus „Kernel-Dump“ ausgewählt. Da der „Kernel-Dump“ keine Informationen über den User-Modus enthält, wird die Ursache des Problems evtl. nicht immer erkannt.
- Abhängig von der Größe des installierten Speichers dauert ein vollständiger Memory Dump länger und hält den Betrieb entsprechend länger auf. Außerdem wird mehr Platz benötigt, um eine Dump-Datei auf der Festplatte zu speichern.

4.10.1.2 Einstellen des Memory Dump

Vollständigen Memory Dump einstellen

Ein vollständiger Memory Dump kann nicht im Fenster für System Dump-Einstellungen gesetzt werden. Um ihn einzustellen, müssen Sie folgenden Wert in der Registry ändern:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\CrashControl
„CrashDumpEnabled“ (type: REG_DWORD, data: 0x1)

Nach Änderung der Einstellung starten Sie das System neu. Einzelheiten zum Sicherungspfad und Überschreib-Einstellungen finden sie unter "Kernel Dump/ Kleinen Dump einstellen."

Kernel Dump/Kleinen Dump einstellen

Gehen Sie wie folgt vor, um die Dump-Datei einzurichten:

1 Melden Sie sich beim Server als Systemverwalter an.

2 Überprüfen Sie den freien Plattenspeicherplatz auf dem Laufwerk, auf dem die Dump-Datei erstellt werden soll.
Weitere Einzelheiten finden Sie in Abschnitt 4.10.1.4, „Paging-Datei einrichten“.

3 Wählen Sie [Start] → [Control Panel] → [System].
Das Dialogfeld [System Property] wird angezeigt.

4 Wählen Sie das Registerblatt [Detail Setting] und klicken Sie auf [Set] bei [Startup and Recovery].
Das Dialogfeld [Startup and Recovery] wird angezeigt.

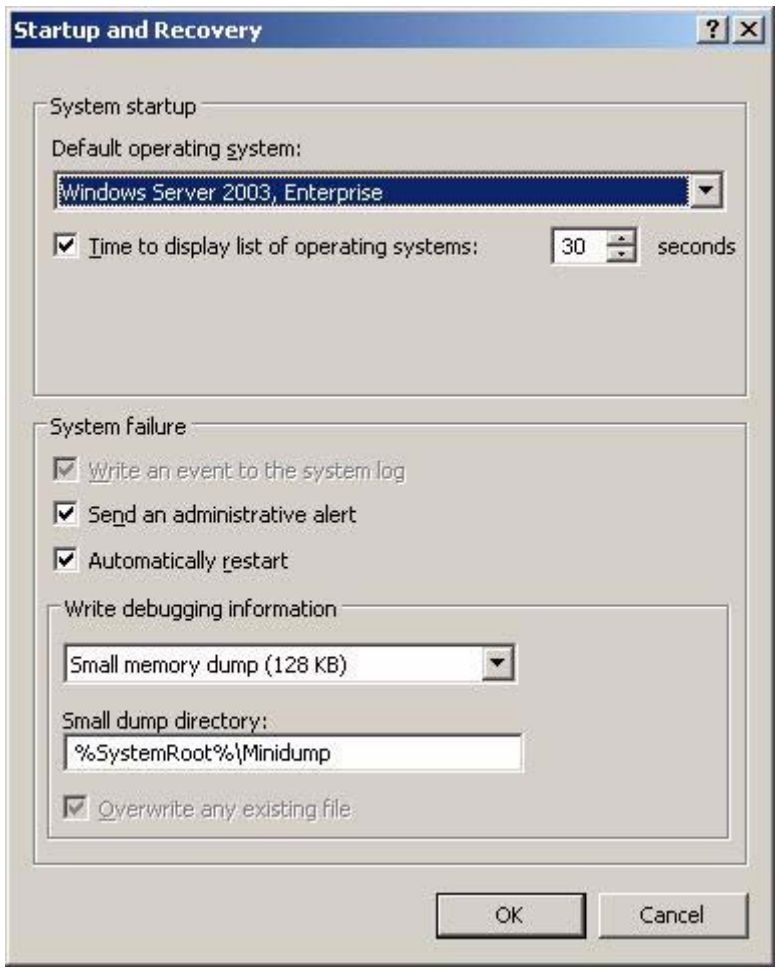


Abbildung 4.53 Das Dialogfeld [Startup and Recovery]

5 Machen Sie die folgenden Einstellungen:
Wählen Sie aus der Dropdown-Liste bei [Write debugging information] den Dump-Typ aus.

- Kernel memory dump (recommended)
  Nur der Inhalt des Kernel wird in die Dump-Datei geschrieben.
  Geben Sie im Feld [Dump file] den vollständigen Pfad des Verzeichnisses an, in dem die Dumpdatei gespeichert werden soll. Wenn das Kontrollkästchen bei [Overwrite any existing file] aktiviert ist, werden Debug-Informationen immer in die angegebene Datei geschrieben.

- Small memory dump (64 KB oder 128 KB)
  Es wird das Minimum an erforderlichen Daten in die Dump-Datei geschrieben. Geben Sie im Feld [Small Dump Directory] den vollständigen Pfad des Verzeichnisses an, in dem kleine Dumps gespeichert werden. Nach jedem nicht wiederherstellbaren Fehler wird in dem hier genannten Verzeichnis eine neue Datei angelegt.

6 Klicken Sie auf [OK], um das Dialogfeld [Startup and Recovery] zu schließen.

7 Klicken Sie auf [OK], um das Dialogfeld [System Property] zu verlassen.

8 Starten Sie das System neu.
Die Einstellungen treten erst nach dem Neustart in Kraft.

4.10.1.3 Überprüfen der Memory Dump-Einstellungen

Führen Sie im voraus einen Memory Dump aus, um sicherzustellen, dass die Speicherinformationen normalerweise aufgezeichnet werden. Messen Sie außerdem die Zeit, bis der Dump wirklich ausgegeben wird und die Zeit für einen Neustart des Systems. Damit können Sie abschätzen, wie viel Zeit bis zur Wiederaufnahme der Geschäfte vergeht. Abhängig vom Ergebnis können Sie überlegen, ob Sie den Dump-Modus benötigen.

Um einen Dump einzurichten, geben Sie INIT als Ziel-Partition an, indem Sie [Partition] - [Power Control] aus dem MMB Web-UI auswählen. Einzelheiten finden Sie im Handbuch *PRIMEQUEST 500A/500/400 Series Reference Manual: Basic Operation/GUI/Commands* (C122-E003EN), Kap. 5 „MMB Web-UI“.

4.10.1.4 Paging-Datei einrichten

Gehen Sie wie im Folgenden beschrieben vor, um die Paging-Datei einzurichten. Sofern nichts Gegenteiliges angegeben wird, können die während der Installation von Windows voreingestellten Werte für die Paging-Datei übernommen werden.

1 Melden Sie sich als Systemverwalter beim Server an.

2 Wählen Sie [Start] → [Control Panel] → [System].
Das Dialogfeld [System Property] wird angezeigt.

3 Wählen Sie das Registerblatt [Detail Setting] und klicken Sie bei [Performance Options] auf [Set].
Das Dialogfeld [Performance Options] wird angezeigt.

4 Wählen Sie das Registerblatt [Advanced].

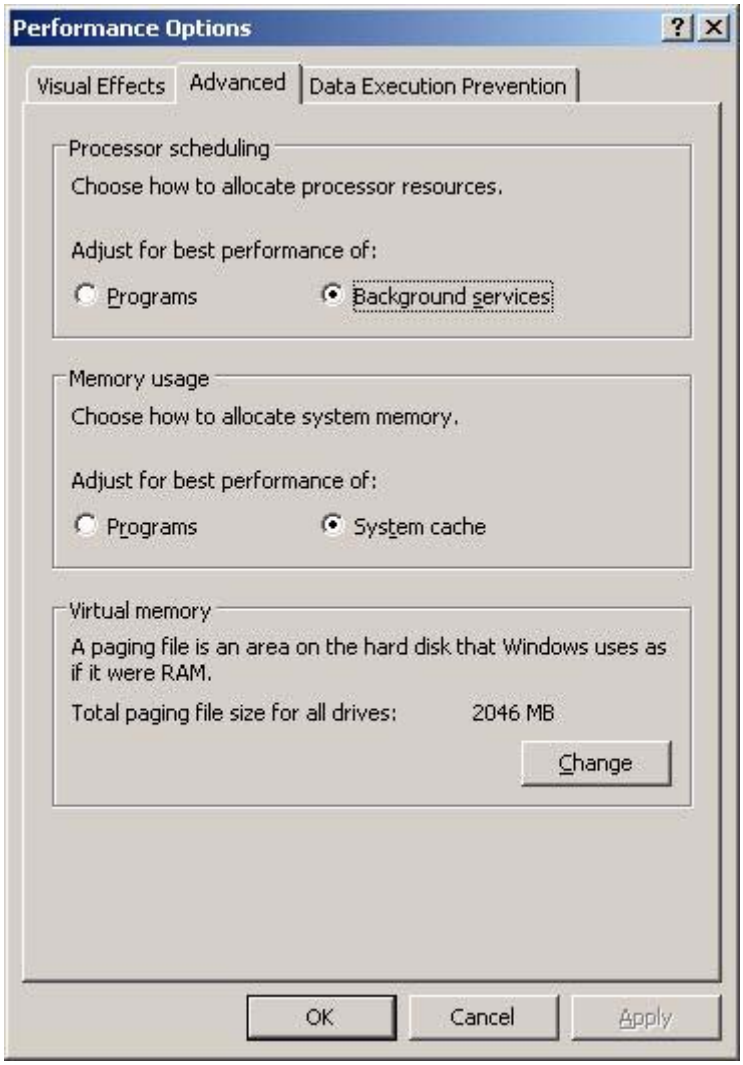


Abbildung 4.54 Das Dialogfeld [Performance Options]

5 Klicken Sie unten im Bereich [Virtual Memory] auf die Schaltfläche [Change]. Das Dialogfeld [Virtual Memory] wird angezeigt.

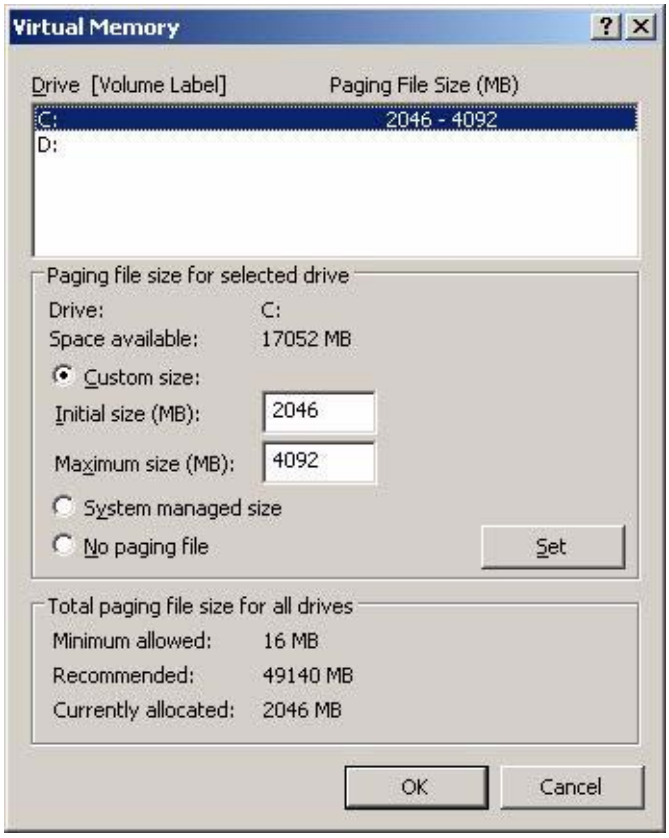


Abbildung 4.55 Das Dialogfeld [Virtual Memory]

6 Legen Sie das Laufwerk fest, auf dem die Paging-Datei angelegt werden soll. Wählen Sie im Feld [Drive] das Laufwerk aus, auf dem das System installiert ist. Im Bereich [Paging file size for selected drive] wird das ausgewählte Laufwerk bei [Drive] angezeigt.

7 Aktivieren Sie das Optionsfeld [Custom size] und geben Sie im Feld [Initial size] einen Wert ein.
Gehen Sie wie folgt vor, um den Mindestwert zu ermitteln:

1 Geben Sie im Feld [Initial size (MB)] unter [Custom size:] den Mindestwert ein (in dem in Abbildung 4.55 dargestellten Dialogfeld [Virtual Memory] ist das der Wert 16 MB, der bei [Minimum allowed:] im Bereich [Total paging file size for all drives] unten angegeben ist). Geben Sie im Feld [Maximum size (MB)] den Mindestwert + 2 MB ein (gemäß den Inhalten des in Abbildung 4.55 dargestellten Dialogfeldes [Virtual Memory] also 18 MB). Klicken Sie dann auf die Schaltfläche [Set].

2 Wenn die unten dargestellte Meldung nicht erscheint, können Sie die eingegebenen Werte beibehalten.
Wenn die unten dargestellte Meldung erscheint, nehmen Sie den in ihr angegebenen Wert als Mindestwert (in diesem Beispiel 200 MB).
Im Allgemeinen empfiehlt es sich, den vom Betriebssystem automatisch zugewiesenen Wert zu übernehmen.

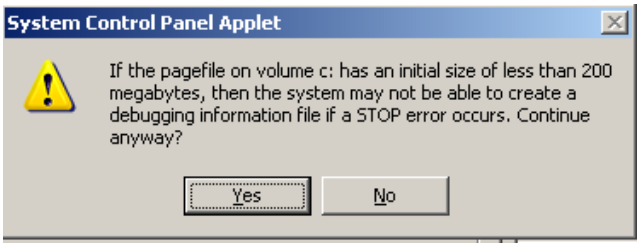

System Control Panel Applet
If the pagefile on volume c: has an initial size of less than 200 megabytes, then the system may not be able to create a debugging information file if a STOP error occurs. Continue anyway?
Yes
No

Abbildung 4.56 Bestätigungsfenster

8 Geben Sie im Feld [Maximum size] einen Wert ein.
Der Wert muss größer sein als der Wert für [Initial size].

9 Speichern Sie die Einstellungen.
Klicken Sie im Bereich [Paging file size for selected drive] auf [Set]. Die Einstellungen werden gespeichert und unter [Paging File Size] bei [Drive] oben im Dialogfeld angezeigt.

10 Klicken Sie auf [OK], um das Dialogfeld [Virtual Memory] zu schließen.

11 Klicken Sie auf [OK], um das Dialogfeld [Performance Options] zu schließen.

12 Klicken Sie auf [OK], um das Dialogfeld [System Property] zu schließen.

13 Starten Sie das System neu.
Die Einstellungen treten nach dem Neustart in Kraft.

4.10.1.5 Hinweis

Wenn die Paging-Datei nicht der System-Partition (normalerweise Laufwerk C) zugewiesen wird, wird bei Auftreten eines Stop-Fehlers keine Dump-Datei erzeugt. Verschieben Sie die Paging-Datei nicht, sofern Sie nicht dazu angewiesen werden.

4.10.2 Präventive Fehlerbehebung mit [DSNAP]

Das Softwareprogramm DSNAP sammelt schnell und zuverlässig Diagnosedaten, wenn im Windows-Betriebssystem ein Fehler auftritt. Wenn auf Ihrem System ein Fehler auftritt, benutzt der Kundendienst-Techniker dieses Programm, um damit Konfiguration und Einstellungen Ihres Systems zu ermitteln und Prozesse zu analysieren.

- Installation

Einzelheiten enthält der Abschnitt 3.3.6, „High Reliability Tools“.

- Verwendung

Näheres finden Sie in der Datei \DSNAP README.TXT auf [BS-Installationslaufwerk].

4.11 NTP-Client einrichten

In diesem Abschnitt wird beschrieben, wie mit NTP (Network Time Protocol) die Systemzeit auf der PRIMEQUEST eingestellt wird kann.

Bei NTP handelt es sich um ein Protokoll, mit dem der Austausch von Zeit-Informationen zwischen einzelnen Rechnern gesteuert wird. NTP synchronisiert die Systemuhr bei Systemstart mit einer präzisen Referenzuhr und hält sie dann in einem bestimmten Genauigkeitsbereich.

4.11.1 NTP-Betrieb bei PRIMEQUEST

In diesen Abschnitt wird beschrieben, wie auf der PRIMEQUEST mit NTP die Systemzeit der einzelnen Partitionen kontrolliert wird.

Die PRIMEQUEST stellt auf dem MMB NTP-Client- und Serverfunktionen bereit. Die NTP-Clientfunktionen des MMB erlauben Ihnen, bis zu drei gesonderte NTP-Server festzulegen. Die Partitionen des Systems benutzt die NTP-Serverfunktion des MMBs, um ihre Partitionszeit anzugleichen.

Das MMB braucht jedoch für den NTP-Server nicht in irgendeiner der Partitionen spezifiziert zu werden. Geben Sie auf dem NTP-Client mehrere NTP-Server an (es werden wenigstens drei empfohlen).

Die folgende Abbildung veranschaulicht eine Konfiguration, in der die anderen NTP-Server benutzt werden.

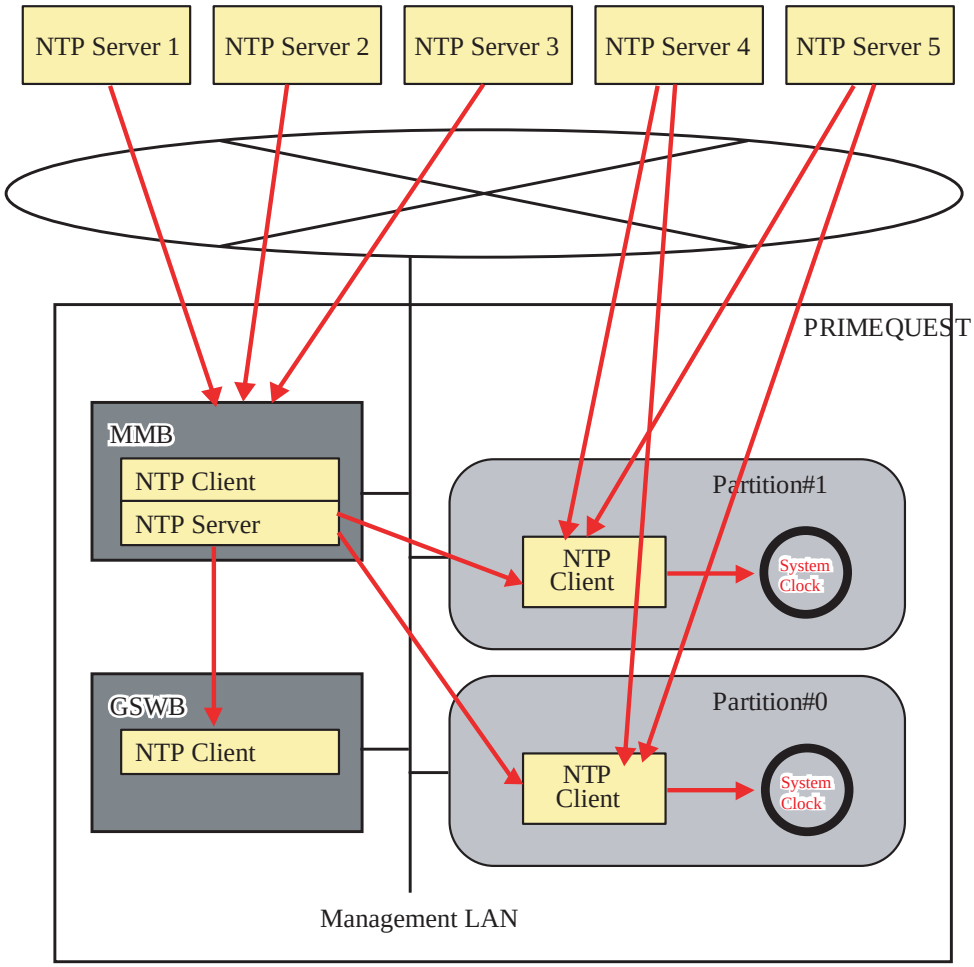


Abbildung 4.57 Konfiguration bei Nutzung externer NTP-Server

Anmerkungen:

- Bei den NTP-Servern 1 bis 5 handelt es sich um NTP-Server mit hochpräzisen Uhren, die mit dem Internet oder dem Intranet verbunden sind.
- Das GSWB ist ausschließlich in den Modellen PRIMEQUEST 580A/540A/540/540/480/440 eingebaut.

4.11.2 NTP-Server einrichten

Richten Sie die NTP-Server ein, wenn dies nicht bereits bei der Initialisierung des MMB geschehen ist.

Benutzen Sie die NTP-Clientfunktion, um die anderen NTP-Server einzurichten, mit denen die Systemzeit synchronisiert wird. Erlauben Sie ferner anderen Clients, das MMB als NTP-Server zu benutzen.

Anm.: Verwenden Sie die folgenden Einstellungen, falls das MMB als NTP Server eingestellt ist und jede Partition innerhalb des Systems als NTP (dies ist jedoch keine typische Konfiguration):

- NTP: Enable
- NTP Server 1 zu NTP Server 3: 0.0.0.0

1 Wählen Sie [Network Configuration] → [Date/Time].
Das Fenster [Date/Time] wird angezeigt.

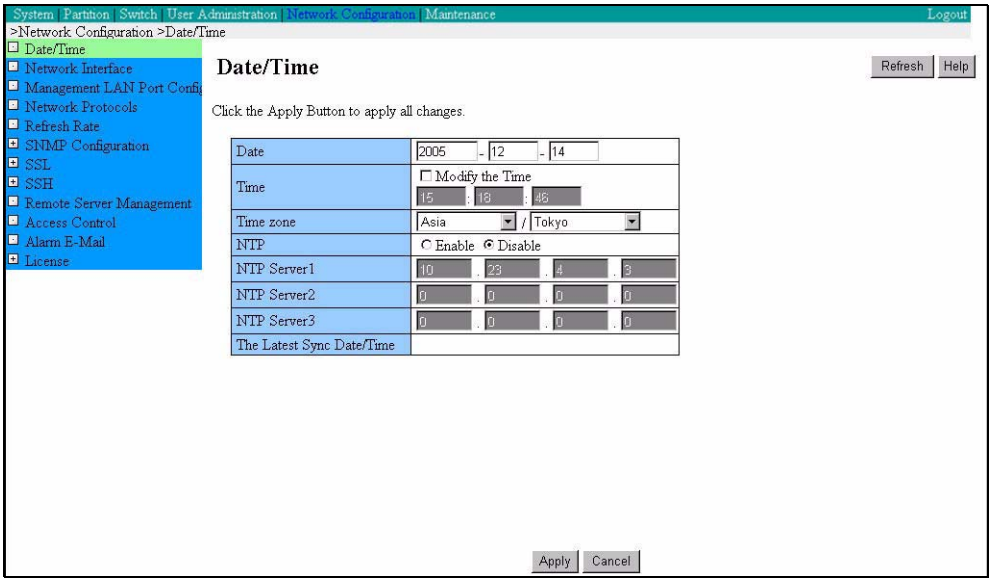


Abbildung 4.58 Das Fenster [Date/Time] (Beispiel)

2 Aktivieren Sie bei [NTP] das Optionsfeld [Enable].

3 Geben Sie die IP-Adresse der anderen NTP-Server an.
NTP Server1: geben Sie den ersten NTP-Server an.
NTP Server2: geben Sie den zweiten NTP-Server an.
NTP Server3: geben Sie den dritten NTP-Server an.

4 Klicken Sie auf [Apply], um die Eingaben zu übernehmen.
Das MMB synchronisiert die Systemzeit mithilfe der in den Feldern [NTP Server1] bis [NTP Server3] angegebenen NTP-Servern. Somit können andere Clients das MMB ihrerseits als NTP-Server benutzen.

5 Warten Sie einige Minuten und klicken Sie dann auf die Schaltfläche [Refresh], um zu prüfen, ob die Systemzeit richtig angezeigt wird.

4.11.3 Partitionen als NTP-Clients einrichten

Wenn der NTP-Server eingestellt wurde übernimmt jede aller Partitionen die Rolle eines NTP-Clients.

4.11.3.1 NTP-Clientbetrieb in einer Linux-Partition

Der NTP-Client wird in den einzelnen Partitionen bei folgenden Aufgaben benötigt:

1 Starten des Linux-Betriebssystems.

2 Synchronisieren der Systemzeit (stufenweise Synchronisierung wird nur verwendet, wenn der NTP-Client erstmals eingesetzt wird) (ntpdate -b).

3 Starten des ntp-Dämons, um die Genauigkeit der Systemzeit aufrecht zu erhalten.

Anm.: In der Regel werden die Schritte 2 und 3 während des Urladevorgangs (IPL) gemäß dem Startskript durchgeführt.

NTP auf einer Partition einrichten

Gehen Sie wie folgt vor, um NTP auf einer Linux-Partition einzurichten:

1 Stellen Sie den NTP-Server in der Datei /etc/ntp.conf wie folgt ein:

/etc/ntp.conf file

```
server MMB-IP-Adresse
```

Abbildung 4.59 Einstellen der IP-Adresse des NTP-Servers (Beispiel)

Da für die Kommunikation zwischen dem MMB und einer Partition keine spezifischen Optionen erforderlich sind, reicht diese Einstellung aus, um ntpd benutzen zu können. Wenn das MMB als NTP-Server verwendet wird, geben Sie für das MMB eine virtuelle IP-Adresse an.
Für einen stabilen NTP-Betrieb werden mindestens drei hochverfügbare NTP-Server einschließlich des MMBs empfohlen.
Hinweise:

- Die Beschreibung oben geht davon aus, dass ntpd bereits installiert ist.
- Das MMB in den Modellen PRIMEQUEST 520A/520/420 verfügt über keine virtuelle IP-Adresse.

2 Starten Sie den Dienst neu.
[Red Hat Enterprise Linux]

```
# service ntpd restart
```

[SUSE Linux Enterprise Server]

```
# /etc/init.d/xntpd restart
```

3 Ändern Sie die Konfiguration des Dienstes.
[Red Hat Enterprise Linux]

```
# chkconfig ntpd on
```

[SUSE Linux Enterprise Server]

```
# chkconfig xntpd on
```

4.11.3.2 NTP in einer Windows-Partition einrichten

In diesem Abschnitt wird beschrieben, wie NTP in einer Windows-Partition eingerichtet wird.

1 Melden Sie sich als Systemverwalter beim System an.
2 Wählen Sie [Control Panel] → [Date and Time].
Das Dialogfeld [Date and Time Property] wird angezeigt.
3 Wählen Sie das Registerblatt [Internet Time] aus.
4 Geben Sie im Eingabefeld [Server:] die virtuelle IP-Adresse des MMB ein und klicken Sie auf [OK]. Das Eingabefeld wird geschlossen.

5 Klicken sie nochmals auf das Registerblatt [Internet Time] im Dialogfeld [Date and Time Property], und anschließend auf [Update Now]. Wurde die Verbindung zum NTP-Server erfolgreich hergestellt, erscheint die Meldung, die in Abbildung 4.60 zu sehen ist und bestätigt, dass die Synchronisierung erfolgreich durchgeführt wurde.

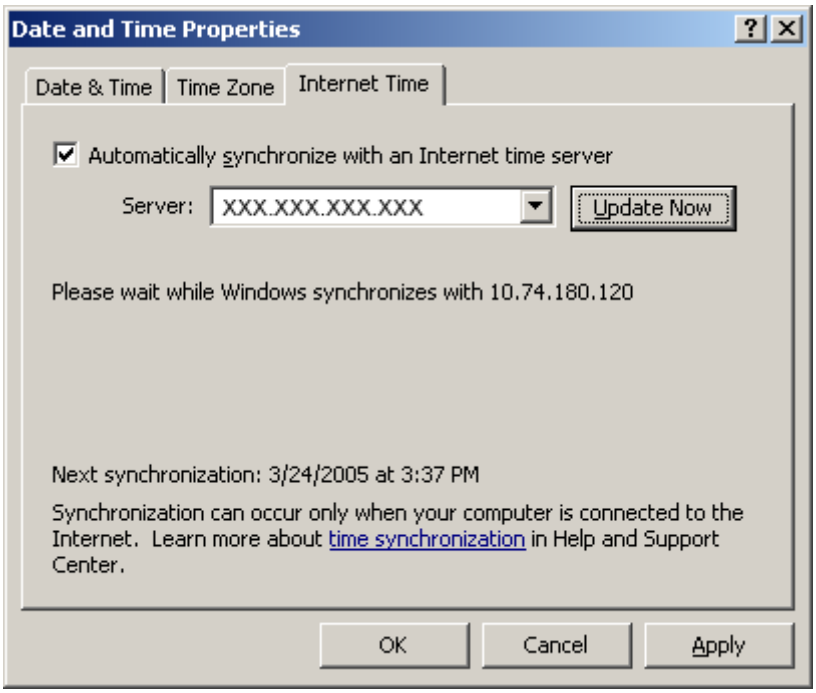

Date and Time Properties
Date & Time
Time Zone
Internet Time
Automatically synchronize with an Internet time server
Server:
XXX.XXX.XXX.XXX
Update Now
Please wait while Windows synchronizes with 10.74.180.120
Next synchronization: 3/24/2005 at 3:37 PM
Synchronization can occur only when your computer is connected to the Internet. Learn more about time synchronization in Help and Support Center.
OK
Cancel
Apply

Abbildung 4.60 Virtuelle IP-Adresse des MMB einstellen (Beispiel)

Hinweise:

1. Wenn das Kontrollkästchen [Automatically synchronize with an Internet time server] aktiviert wurde, erfolgt die Synchronisierung des MMB mit dem angegebenen NTP-Server automatisch.
2. Im Feld [Server:] ist „time.windows.com“ als NTP-Server voreingestellt.
3. Wenn die Synchronisierung mit dem NTP-Server nicht gelingt, erscheint in der Ereignislogdatei ein Win32Time-Fehler.
4. In der Kommunikation mit einem externen NTP-Server wird die physikalische Adresse des MMB verwendet. Falls für die Kommunikation Einstellungen wie z. B. die der Firewall geändert werden müssen, muss berücksichtigt werden, dass nicht nur die virtuelle IP-Adresse (Virtual IP address) erreicht werden muss, sondern auch die Physikalischen IP-Adressen der MMBs (MMB#0 IP address and MMB#1 IP address).
5. Wird innerhalb von drei Minuten nach der in Abschnitt 4.11.2, „NTP-Server einrichten“ beschriebenen Prozedur [Update Now] angeklickt, kann die Synchronisierung fehlschlagen. Warten Sie in diesem Fall mindestens drei Minuten und klicken sie dann nochmal [Update Now].

6 Klicken Sie auf [OK], um die Einstellungen zu speichern.

4.11.3.3 NTP-Einstellung für eine Partition, die zu einer Domain gehört

Falls eine Partition, in der Windows installiert ist, zu einer Domain gehört (sie ist dann Mitglied dieser Domain), wird die Zeiteinstellung der Partition automatisch mit dem NTP-Server des Domain Controllers synchronisiert. In diesem Fall wird Reiter [Internet Time] wie in der folgenden Abbildung nicht angezeigt.

Jede Partition in einer MSCS-Cluster-Umgebung muss immer zu einer Domain gehören, und die Zeiteinstellungen der Partitionen werden automatisch mit dem NTP-Server des Domain Controllers synchronisiert.

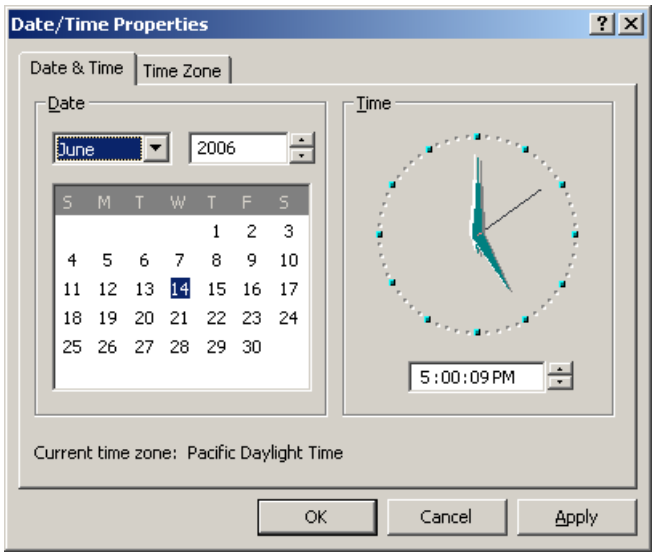


Abbildung 4.61 Dialogbox [Date and Time Properties] (bei Zeitsynchronisation mit einem NTP-Server)

4.12 Betriebssystem sichern

In diesem Abschnitt wird beschrieben, wie Sie Ihr Linux (Red Hat)- oder Windows-Betriebssystem sichern. Einzelheiten zu einer Wiederherstellung des Systems finden Sie im Kapitel 1, „System Maintenance“ des *PRIMEQUEST 500A/500/400 Series Reference Manual: Tools/Operation Information* (U41757-J-Z816-x-76, C122-E074EN).

- Linux (Red Hat) sichern (→ 4.12.1)
- Windows-Partitionen sichern (→ 4.12.2)

4.12.1 Linux (Red Hat) sichern

In diesem Abschnitt wird beschrieben, wie Sie die Systemdatenträger einer Linux-Partition sichern. Es stehen zwei Sicherungsverfahren zur Wahl:

- mit Standard-Utilities des Betriebssystems
- mit SystemcastWizard Lite

Die im Folgenden beschriebenen Verfahren zur Sicherung von Linux-Systemdatenträgern verwenden die jeweiligen Standard-Utilities für den Betrieb

- ohne PRIMECLUSTER GDS
- mit PRIMECLUSTER GDS

Hinweis: Bereiten Sie eine Einheit, z.B. eine Bandeinheit als Sicherungsgerät vor.

Anm.: Führen Sie die Sicherung/Wiederherstellung auf der Betriebssystemkonsole aus. Es eignet sich eine KVM-Konsole oder eine serielle Konsole.

Einzelheiten über die Verwendung des SystemcastWizard Lite für eine Linux-Sicherung finden Sie im *PRIMEQUEST SystemcastWizard Lite User's Guide* (C122-E010EN).

4.12.1.1 Sicherung ohne PRIMECLUSTER GDS

In diesem Abschnitt wird beschrieben, wie eine Sicherung durchgeführt wird, wenn PRIMECLUSTER GDS nicht eingesetzt wird.

Das folgende Beispiel geht von der folgenden Laufwerkskonfiguration aus:

```
/dev/sda1 : /boot/efi
/dev/sda2 : /
/dev/sda3 : swap
/dev/sda4 : /work
```

Vorbereitung

Überprüfen Sie zunächst die Betriebsumgebung (System- und Laufwerkskonfiguration) des zu sichernden Systems.

Hinweis: Diese Angaben werden für eine Wiederherstellung benötigt, wenn das Laufwerk ausfallen sollte. Sichern Sie die Angaben, damit sie im Falle einer Wiederherstellung zur Verfügung stehen.

(1) Systemkonfiguration überprüfen

1 Überprüfen Sie die IDE- und SCSI-Kartentypen sowie den IRQ- und E/A-Port-Status.

```
# dmesg
```

oder

```
# more /var/log/messages
```

2 Überprüfen Sie die Treiberdateien.

```
# lsmod
```

3 Überprüfen Sie die Gerätenamen, -typen sowie die Höchst- und Niedrigstwerte.

```
# ls -al /dev/sda*
```

(2) Laufwerkskonfiguration überprüfen

1 Überprüfen Sie den Mount-Status.

```
# cat /etc/fstab
```

2 Speichern sie die Partitionskonfigurationen.
Im Falle z.B. eines Plattenfehlers kann die Wiederherstellung auf einer neuen Platte erforderlich sein.
Entsprechend muss das Kommando „parted“ verwendet werden, um die aktuelle Partitionskonfiguration festzuhalten und die Wiederherstellung vorzubereiten.
Unten sehen Sie ein Beispiel für die gespeicherten Informationen.
Beispiel:

```
# parted
(parted) unit s
(parted) print

Disk /dev/sdb: 71390319s
Sector size (logical/physical): 512B/512B
Partition table: gpt

 No.      Start          End            Size         File system     Name      Flag
  1       34s            204833s        204800s      fat16           Primary   msftres
  2       204834s        42147873s      41943040s    ext2            Primary
  3       42147874s      46228383s      4080510s     linux-swap      Primary
  4       46228384s      67199903s      20971520s    ext2            Primary
(parted) quit
```

Anm.: Bei RHEL5 (IPF) gibt das Unterkommando „print“ des Kommandos „parted“ vereinfachte Werte mit Einheiten wie „MB“ hinter den Werten aus. Deswegen können die Werte erheblich von den wirklichen Größen abweichen.
Um die zum Zeitpunkt des Backups ausgegebenen Größenunterschiede zu minimieren, geben sie als Ausgabeeinheit eine kleinere Maßeinheit an, bevor Sie das Unterkommando „print“ ausführen und speichern Sie es für die Partitionsrekonfiguration.
Im obigen Beispiel wird „unit s“ als Ausgabeeinheit (s) für Sektoren verwendet.

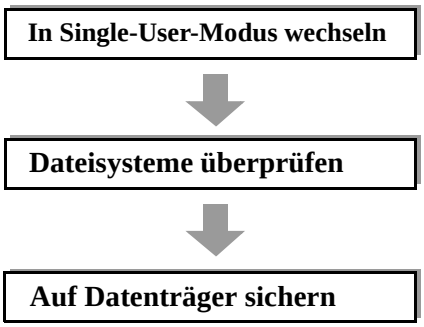
3 Überprüfen Sie die Labelnamen der Dateisysteme.

```
# e2label /dev/sda2
```

* Wenn ein in /boot/efi eingehängtes Gerät angegeben wird, tritt ein Fehler auf, da es sich um ein anderes Dateisystem handelt. Das verursacht jedoch kein Problem, da „boot/efi“ nicht als Label-Name nicht angegeben ist. Eine Überprüfung ist nicht erforderlich.

Sicherung

Gehen Sie bei der Sicherung wie folgt vor.



In den folgenden Abschnitten werden die einzelnen Schritte genauer beschrieben.

(1) In Single-User-Modus wechseln

Zur Durchführung einer Sicherung müssen sämtliche Prozesse deaktivieren werden, die nicht für die Sicherung benötigt werden, damit Datenkonsistenz gewährleistet ist. Wechseln Sie hierzu in den Single-User-Modus.

- Bei laufendem System
  1. Mit root-Berechtigung anmelden
  2. Alle Anwendungen beenden
  3. In den Single-User-Modus wechseln (Run Level 1).

```
# init 1
```

- Bei ausgeschaltetem System
  1. System starten

     Wenn das Menü des EFI Boot Managers erscheint, geben Sie den Namen des Betriebssystems ein, das gestartet werden soll (z.B. Red Hat Enterprise Linux).

     Hinweis: Hierzu sind erweiterte Einstellungen erforderlich. Einzelheiten finden Sie im Abschnitt 5.3.8.2, „[Boot Control] window“ des *PRIMEQUEST 500A/500/400 Series Reference Manual: Basic Operation/ GUI/Commands* (U41633-J-Z816-x-76/C122-E003EN).
  2. Geben Sie nach dem Prompt „ELILO boot:“ das unten angegebene Kommando ein.
     - bei Verwendung einer KVM-Konsole

```
kernel-label-name 1
```

     - bei Verwendung einer seriellen Konsole

```
kernel-label-name 1 console=ttyS0,19200n8r
```

     Wenn der Single-User-Modus aktiviert ist, erschein im Command Line Interface ein Prompt.

     Hinweis: Den aktuellen Wert für *kernel-label-name* finden Sie in der folgenden config-Datei:
     /boot/efi/efi/redhat/elilo.conf

(2) Dateisystem überprüfen

Überprüfen Sie das zu sichernde Dateisystem.

Das zu sichernde Dateisystem heißt ext3 (oder ext2). „/boot/efi“ und Swap müssen nicht überprüft werden.

- Wenn sich das Dateisystem nicht unter „/“ (root), „/boot/efi“ oder Swap befindet:

  1 Hängen Sie das zu sichernde Dateisystem aus.

```
# cd /
# umount /work
```

  2 Überprüfen Sie das Dateisystem.

```
# e2fsck -pfv /dev/sda4
```

  Hinweis: Führen Sie das Kommando e2fsck nicht aus, wenn das Kommando umount einen Fehler gemeldet hat.
  Wenn das Kommando e2fsck ausgeführt wird, während das Dateisystem noch gemountet ist, könnte es zu Datenverlusten kommen.

- Wenn sich das Dateisystem unter „/“ (root) befindet:

  1 Hängen Sie das Dateisystem „/“ im Lesemodus um.

```
# mount -r -n -o remount /
```

  2 Stellen Sie sicher, dass das Dateisystem konsistent ist.

```
# e2fsck -pfv /dev/sda2
```

  3 Hängen Sie das Dateisystem im normalen Modus wieder ein.

```
# mount -w -n -o remount /
```

  Hinweis: Führen Sie das Kommando e2fsck nicht aus, wenn das Dateisystem nicht im Lesemodus eingehängt werden kann.
  Wenn das Kommando e2fsck ausgeführt wird, während das Dateisystem noch im Schreibmodus eingehängt ist, könnte es zu Datenverlusten kommen.

(3) Sicherung auf einem Datenträger

Führen Sie für jede Partition des Laufwerks eine Sicherung auf einen Datenträger aus. Für die Datensicherung wird das Kommando dump verwendet. Es unterstützt jedoch nur die Dateisysteme ext2 und ext3. Benutzen Sie das Kommando tar, um /boot/efi eines anderen Dateisystems zu sichern.

Hinweis: Achten Sie darauf, dass die Blockgröße der verwendeten Bänder bei Sicherungen und Wiederherstellungen gleich ist. Die Wiederherstellung schlägt fehlt, wenn die bei der Wiederherstellung benutzte Blockgröße von der Blockgröße der Sicherung abweicht.

- Lokale Bandeinheit:

  1 Bandeinheit vorbereiten.
  Näheres finden Sie im Handbuch zum Kommando „mt“.

  - Rufen Sie den Status der Bandeinheit ab.

```
# mt -f /dev/nst0 status
```

  - Spulen Sie das Band zurück.

```
# mt -f /dev/nst0 rewind
```

  2 Sicherung durchführen.

  - Bei Dateisystemen außer /boot/efi
    Benutzen Sie das Kommando dump für die Sicherung.

```
# dump 0uf /dev/nst0 /dev/sda2
```

  - Bei /boot/efi
    Benutzen Sie das Kommando tar für die Sicherung.

```
# cd /boot/efi
# tar czvf /dev/nst0
```

- Entfernte Bandeinheit:

  1 Starten Sie das Netzwerk.

```
# /etc/rc.d/init.d/network start
```

  2 Aktivieren Sie das Netzwerk.

```
# ifconfig eth0 xxx.xxx.xxx.xxx netmask xxx.xxx.xxx.xxx
broadcast\
xxx.xxx.xxx.xxx
```

\:zeigt an, dass kein Zeilenumbruch eingefügt werden soll.

Anm.: Setzen Sie die für Ihr System zutreffenden Werte und Adressen ein.

3 Bandeinheit vorbereiten.

Benutzen Sie das Kommando mt mit ssh, wenn Sie die Sicherung auf einer entfernten Bandeinheit erstellen.

Näheres finden Sie im Handbuch zum Kommando „mt“.

- Band zurückspulen.

```
# ssh remote-host-name mt -f /dev/nst0 rewind
```

Geben Sie das Kennwort ein, wenn es angefordert wird.

4 Sicherung durchführen.

Benutzen Sie für die Sicherung das Kommando ssh.

- Bei Dateisystemen außer /boot/efi

  Benutzen Sie das Kommando dump für die Datensicherung.

```
# dump 0f - /dev/sda2 | ssh remote-host-name dd of=/dev/nst0
```

Geben Sie das Kennwort ein, wenn es angefordert wird.

- Bei /boot/efi

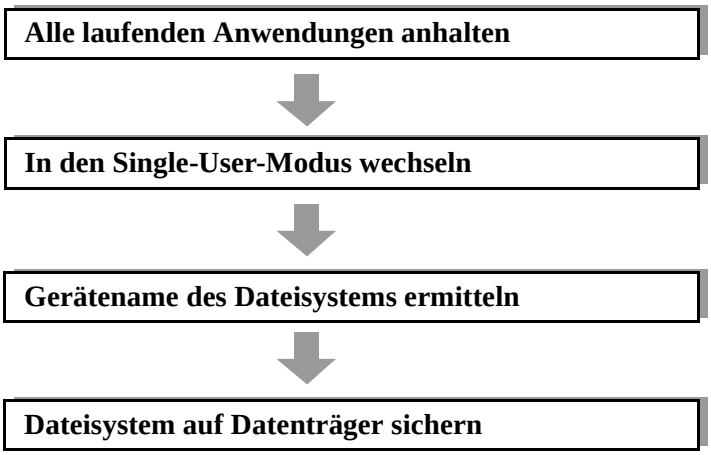
  Benutzen Sie das Kommando tar für die Datensicherung.

```
# cd /boot/efi
# tar czvf - . | ssh remote-host-name dd of=/dev/nst0
```

Geben Sie das Kennwort ein, wenn es angefordert wird.

4.12.1.2 Datensicherung mit PRIMECLUSTER GDS

Wenn Sie GDS benutzen, führen Sie die Datensicherung wie folgt durch:


Alle laufenden Anwendungen anhalten
In den Single-User-Modus wechseln
Gerätename des Dateisystems ermitteln
Dateisystem auf Datenträger sichern

Anm.: Weitere Informationen enthält das Handbuch *PRIMECLUSTER Global Disk Services*.

4.12.2 Windows-Partitionen sichern

Benutzen Sie SystemcastWizard Lite, um eine Windows-Partition zu sichern.

Weitere Informationen enthält das *PRIMEQUEST SystemcastWizard Lite User's Guide* (C122-E010EN).

4.13 Konfigurationsdaten sichern

In diesem Abschnitt wird beschrieben, wie Sie die Konfigurationsdaten sichern.

- PSA-Konfigurationsdaten sichern (→ 4.13.1)
- EFI-Konfigurationsdaten sichern (→ 4.13.2)

Anm.: Sichern Sie die PSA-Einstellungen und die EFI-Konfigurationsinformationen in regelmäßigen Abständen, nachdem Sie das System in Betrieb genommen haben.

4.13.1 PSA-Konfigurationsdaten sichern

Benutzen Sie die Exportfunktion, um die Snapshot-Informationen des PSA in das CSV-Format zu konvertieren und sie im Partitionsverwaltungsbereich zu speichern.

Der Export kann entweder manuell oder automatisch erfolgen. Ein manueller Export wird im Export-Fenster durchgeführt.

Mit der Export-Funktion können bis zu 100 Datendateien gesichert werden. Wenn diese Anzahl erreicht ist, werden die ältesten Dateien gelöscht.

Exportierte Daten bleiben erhalten, bis die maximale Anzahl Dateien erreicht ist oder bis sie vom Systemverwalter gelöscht werden.

4.13.1.1 Exportierte Dateien auflisten

In diesem Abschnitt werden die Funktionen beschrieben, die aus einer Dateiliste heraus vorgenommen werden können.

Folgende Operationen können aus der Listenanzeige heraus durchgeführt werden:

- Schnappschuss im CSV-Format in einer Datei sichern
  Ein im PSA erstellter Schnappschuss kann im CSV-Format in einer Datei gesichert werden.
- Exportierte Datei auf ein Terminal herunterladen
  Eine exportierte Datei kann zu einem Terminal heruntergeladen werden.
- Exportierte Datei löschen
  Eine exportierte Datei kann aus dem Verwaltungsbereich der Partition gelöscht werden.

Anm.: Näheres über das Löschen von Dateien finden Sie im *PRIMEQUEST 500A/500/400 Series Reference Manual: Basic Operation/GUI/Commands* (U41633-J-Z816-x-76/C122-E003EN).

Vorgehensweise

1 Wählen Sie [Partition] → [Partition#x] → [PSA] → [Export List].
Das Fenster [Export List] wird angezeigt.

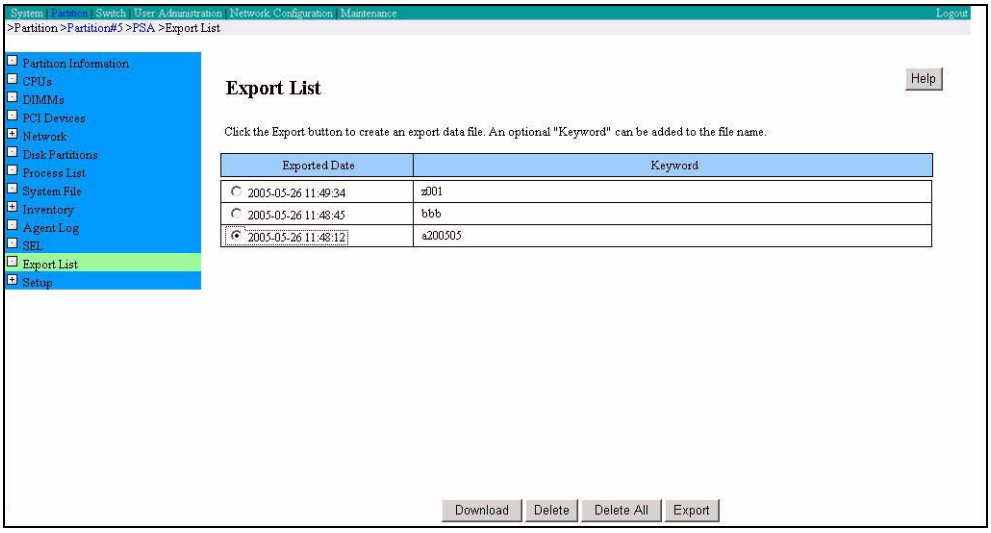


Abbildung 4.62 Das Fenster [Export List] (Beispiel)

2 Aktivieren Sie das betreffende Kontrollkästchen.
Klicken Sie auf die Schaltfläche [Export], um einen Schnappschuss im CSV-Format in eine Datei zu sichern.
Aktivieren Sie das Optionsfeld der Zieldatei und klicken Sie auf die Schaltfläche [Download], um eine exportierte Datei zu einem Terminal herunterzuladen. Es können nicht mehrere Dateien gleichzeitig gewählt werden.
Klicken Sie auf die Schaltfläche [Delete All], um alle exportierten Dateien zu löschen. Aktivieren Sie das Optionsfeld einer Zieldatei und klicken Sie auf die Schaltfläche [Delete], um eine spezifische Datei zu löschen. Es können nicht mehrere Dateien gleichzeitig ausgewählt werden.
Das weitere Vorgehen ist im Abschnitt 4.13.1.2, „In eine CSV-Datei sichern“ beschrieben.

Tabelle 4.8 Elemente des [Export]-Fensters

Feld	Beschreibung
Exported Date	Aktivieren Sie das Optionsfeld der Datei, die exportiert oder gelöscht werden soll. Datum und Uhrzeit der Erstellung der Datei wird im Format jjjj-MM-tt angezeigt. Als Zeit wird die lokale Uhrzeit der Partition zugewiesen.
Keyword	Das für den Export eingegebene Schlüsselwort wird angezeigt. Beim automatischen Export kann kein Schlüsselwort eingegeben werden.

4.13.1.2 In eine CSV-Datei sichern

In diesem Abschnitt wird beschrieben, wie ein im PSA erstellter Schnappschuss in eine Datei im CSV-Format gesichert wird.

Klicken Sie dazu auf die Schritt 2 in Abschnitt 4.13.1.1, „Exportierte Dateien auflisten“ beschriebenen Schaltfläche [Export].

Vorgehensweise

1 Geben Sie das Schlüsselwort ein und klicken Sie auf die Schaltfläche [Export]. Wenn der Vorgang erfolgreich beendet ist, wird das Fenster [Export List] wieder angezeigt.

Anm.: Das Schlüsselwort (Keyword) ist eine den exportierten Daten zusätzlich zugewiesene Bezeichnung, die bis zu 50 Zeichen lang sein kann. Eine Eingabe im Feld [Keyword] ist optional.

Zulässige Zeichen: alphanumerische Zeichen, Leerzeichen und Sonderzeichen (außer < >%&”,\)

Wenn der Exportvorgang fehlschlägt, wird das Dialogfeld [Export Failure Notice] angezeigt. Klicken Sie auf die Schaltfläche [Return]. Das Fenster [Export List] wird mit der zuletzt dargestellten Liste wieder angezeigt.

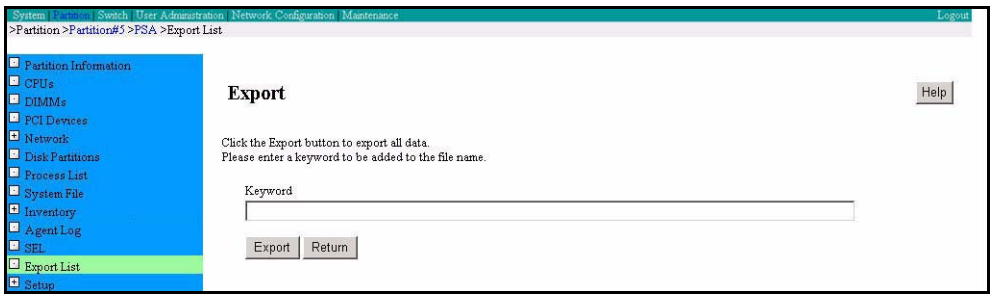


Abbildung 4.63 Das Fenster [Export] (Beispiel)

2 Falls der Export fehlschlägt, klicken Sie auf die Schaltfläche [OK] im Dialogfeld [Export Failure Notice]. Das Fenster [Export List] wird wiederhergestellt, und die Liste spiegelt den aktuellen Stand wider.

4.13.2 EFI-Konfigurationsdaten sichern

Sichern Sie die EFI-Konfigurationsdaten auf einem entfernten PC.

Vorgehensweise

1 Wählen Sie [Maintenance] → [Backup/Restore Configuration] → [Backup EFI Configuration].
Das Fenster [Backup EFI Configuration] wird angezeigt.

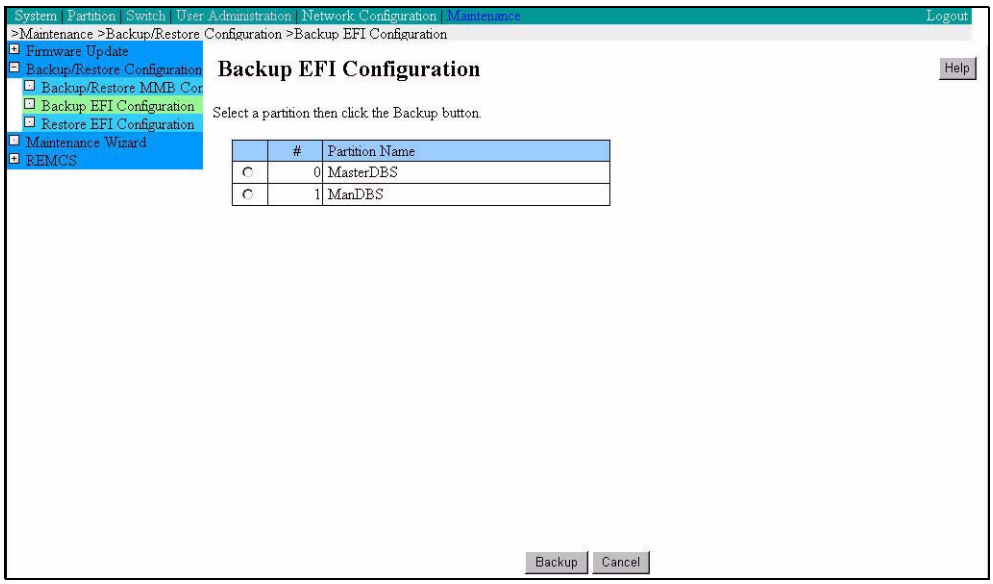


Abbildung 4.64 Das Fenster [Backup EFI Configuration] (Beispiel)

2 Aktivieren Sie das Optionsfeld der Partition, für die die Konfigurationsdaten gesichert werden sollen, und klicken Sie dann auf die Schaltfläche [Backup].

3 Es erscheint ein Dialogfeld, im dem Sie das Ziel festlegen können. Wählen Sie den Zielpfad aus und klicken Sie auf die Schaltfläche [OK].
Der Standardname der zu sichernden EFI-Konfigurationsdatei lautet:

partitionsnummer_backup-datum_efi-version.dat

4 Klicken Sie auf [OK].
Die Konfigurationsdatei wird heruntergeladen.

KAPITEL 5 Systemsicherheit

5.1 Sicherheitseinstellungen

In diesem Kapitel werden Einstellungen beschrieben, die die Sicherheit und das Fehlermeldewesen betreffen.

Führen Sie die für Ihre Betriebsumgebung erforderlichen Sicherheitseinstellungen durch.

Es wird empfohlen, die Einstellungen zu sichern, nachdem Sie die im Folgenden beschriebenen Aufgaben abgeschlossen haben. Eine Beschreibung der Sicherung finden Sie im Abschnitt 2.6, „Konfiguration sichern“.

- Zugriffskontrolle einstellen (→ 5.1.1)
- SNMP einrichten (→ 5.1.2)
- SSH-Parameter festlegen (→ 5.1.3)
- HTTPS-Parameter festlegen (→ 5.1.4)

5.1.1 Zugriffskontrolle einstellen

Die Zugriffskontrolle für ein Netzwerkprotokoll wird aktiviert, um die Sicherheit des MMB zu gewährleisten.

Es wird empfohlen, die Zugriffskontrolle aus Sicherheitsgründen bereits während der Installation einzustellen. Diese Aufgabe kann jedoch auch zu einem späteren Zeitpunkt noch durchgeführt werden.

Filter auswählen

- Vorgehensweise

1 Wählen Sie [Network Configuration] → [Access Control].
Das Fenster [Access Control] wird angezeigt.

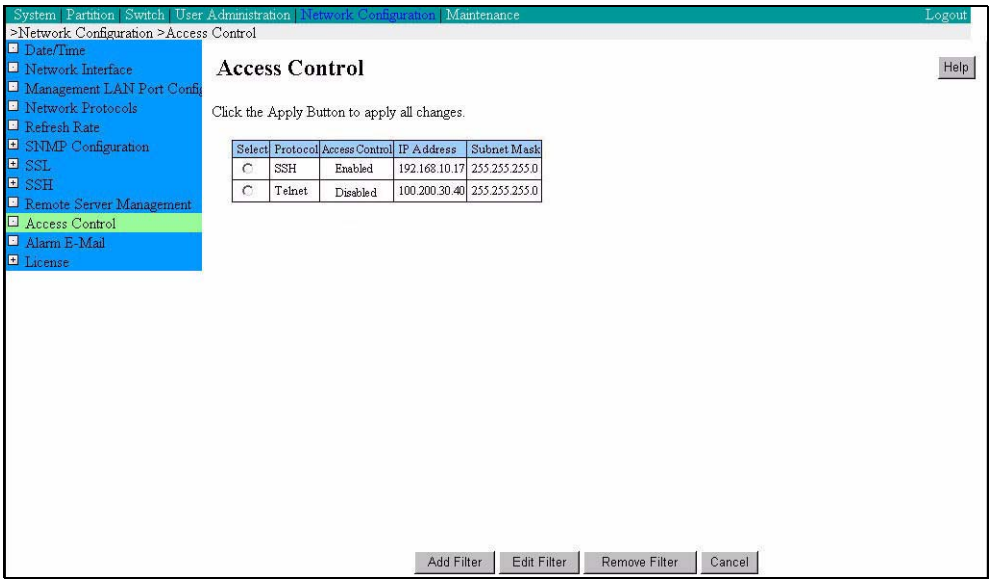


Abbildung 5.1 Das Fenster [Access Control] (Beispiel)

2 Aktivieren Sie das Optionsfeld vor dem Filter, den Sie bearbeiten wollen.

Tabelle 5.1 Ein- und Ausgabe von Daten im Fenster [Access Control]

Feldname	Beschreibung
Protocol	Name des Protokolls: HTTP, HTTPS, Telnet, SSH, SNMP
Access Control	Die Zugangskontrolle kann ein- oder ausgeschaltet werden.
IP Address	IP-Adresse
Subnet Mask	Teilnetzmaske der IP-Adresse

Filter hinzufügen und bearbeiten

- Vorgehensweise

1 Klicken Sie auf die Schaltfläche [Add Filter] im Fenster [Access Control], um einen Filter hinzuzufügen. Klicken Sie auf die Schaltfläche [Edit Filter], um den Filter zu bearbeiten.
Es wird das Fenster [Add Filter] bzw. [Edit Filter] angezeigt.
Das folgende Beispiel zeigt das Fenster [Edit Filter].

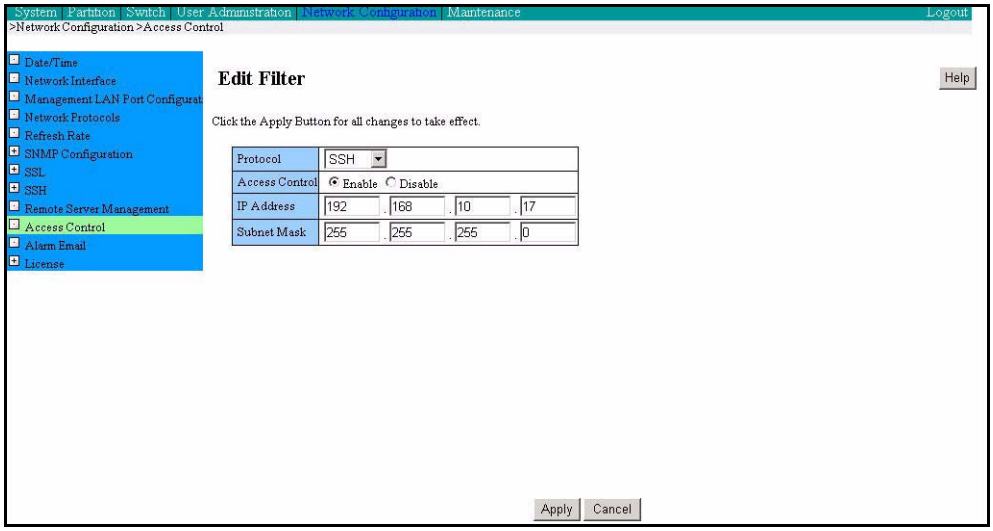


Abbildung 5.2 Das Fenster [Edit Filter] (Beispiel)

2 Machen Sie die erforderlichen Eingaben.
Es können maximal 64 Filter eingestellt werden.
Anmerkung: Beachten Sie die Proxy-Konfiguration, wenn Sie auf Ihrem Arbeitsplatzrechner im Web-Browser einen Proxy einstellen.

Tabelle 5.2 Ein- und Ausgabe von Daten im Fenster [Edit Filter]

Feld	Beschreibung
Protocol	Legt das Protokoll fest, das gefiltert wird. Wählen Sie aus dem Dropdown-Menü ein Protokoll aus: HTTP, HTTPS, Telnet, SSH, SNMP
Access Control	Aktivieren bzw. deaktivieren Sie die Zugangskontrolle mit dem Optionsfeld [Enable] bzw. [Disable]. • Wenn Sie [Disable] wählen, kann das zuvor gewählte Protokoll auf allen IP-Adressen benutzt werden. In diesem Fall sind die Felder [IP Address] und [Subnet Mask] deaktiviert. • Wenn Sie [Enable] wählen, können Sie über die Felder [IP Address] und [Subnet Mask] eine IP-Adresse für das Protokoll festlegen.
IP Address	Zugelassene IP-Adresse Beispiel: 192.168.0.0
Subnet Mask	Teilnetzmaske für die zugelassene IP-Adresse Beispiel: 225.225.225.0

3 Klicken Sie auf [Apply], um die Eingaben zu übernehmen.

Filter löschen

1 Wählen Sie einen Filter und klicken Sie dann auf die Schaltfläche [Remove Filter]. Sie werden aufgefordert, die Aktion zu bestätigen.

2 Klicken Sie auf [OK], wenn Sie den Filter wirklich löschen wollen.
Das Fenster [Access Control] erscheint wieder, und der Filter ist in der Liste nicht mehr enthalten.

Klicken Sie auf die Schaltfläche [Cancel], um den Löschvorgang abzubrechen.

5.1.2 SNMP einrichten

Richten Sie SNMP (Simple Network Management Protocol) ein. Dazu benötigen Sie Systemverwalterberechtigungen. Legen Sie fest, ob während des Betriebs auftretende Fehler an die Verwaltungssoftware gemeldet werden sollen. Legen Sie das Ziel für die Benachrichtigungen fest. Folgende Arbeitsschritte sind erforderlich:

- SNMP aktivieren
- SNMP einstellen
- Ziel für SNMP-Traps einstellen
- SNMP V3-Einstellungen vornehmen

SNMP aktivieren

- Vorgehensweise

1 Wählen Sie [Network Configuration] → [Network Protocols]
Das Fenster [Network Protocols] wird angezeigt.

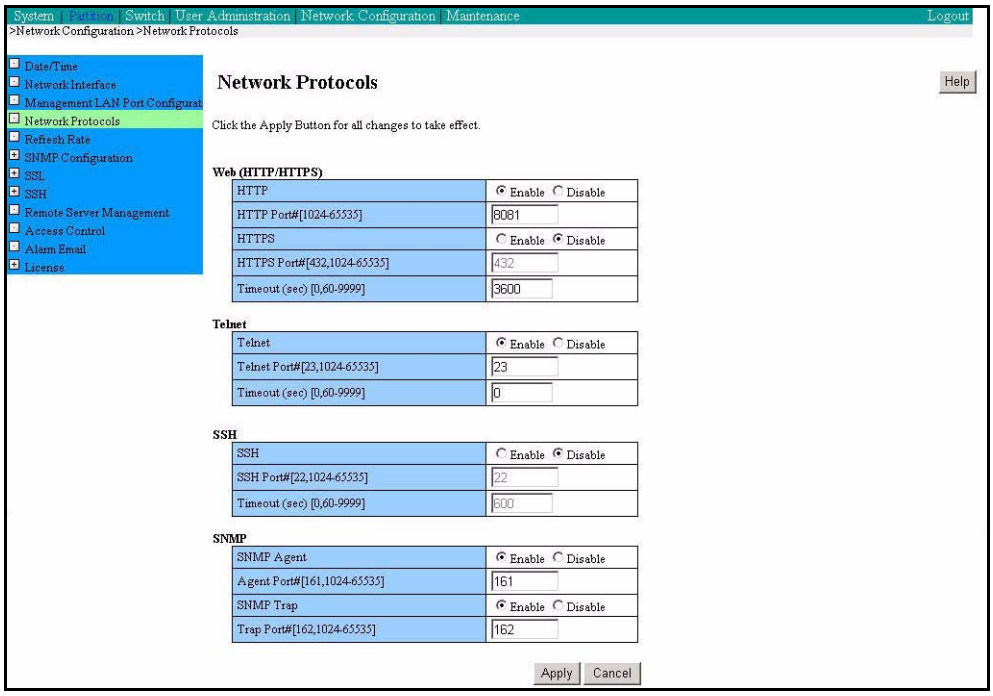


Abbildung 5.3 Das Fenster [Network Protocols] (Beispiel)

2 Machen Sie unter [SNMP] die erforderlichen Angaben.

Tabelle 5.3 Ein- und Ausgabe von Daten im Fenster [Network Protocols]

Feld	Beschreibung
<SNMP>	
SNMP Agent	SNMP Agent aktivieren bzw. deaktivieren. Voreinstellung: Disable
Agent Port	Legt den Port für den SNMP Agent fest. Zugelassene Portnummern sind 161 und 1.024 bis 65.535. Voreinstellung: 161
SNMP Trap	SNMP Trap aktivieren bzw. deaktivieren. Voreinstellung: Disable
Trap Port	Port für SNMP Trap festlegen. Zugelassene Portnummern sind 162 und 1.024 bis 65.535. Voreinstellung: 162

3 Klicken Sie auf [Apply], um die Eingaben zu übernehmen.

SNMP einstellen

- Vorgehensweise

1 Wählen Sie [Network Configuration] → [SNMP Configuration] → [Community]. Das Fenster [SNMP Community] wird angezeigt.

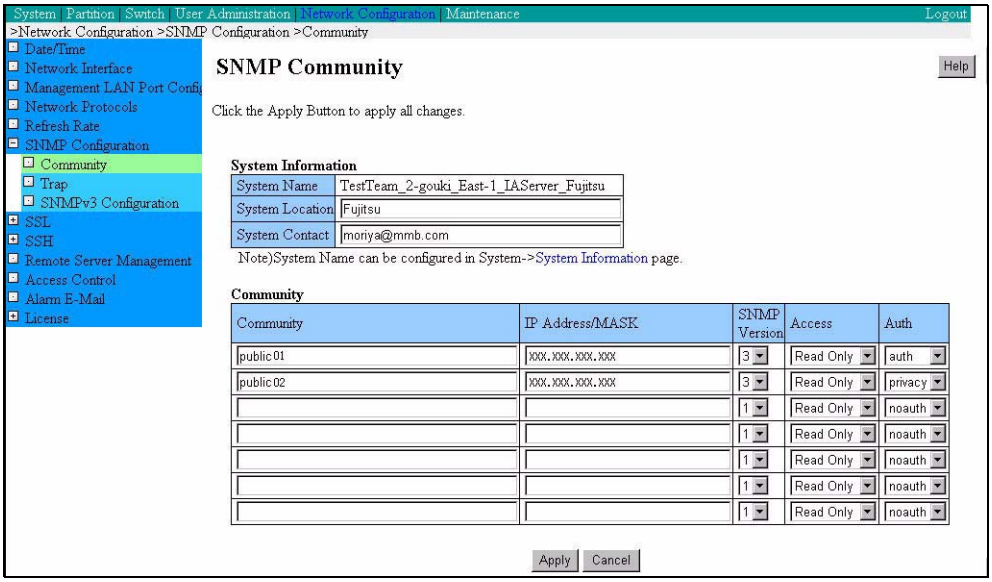


Abbildung 5.4 Das Fenster [SNMP Community] (Beispiel)

2 Machen Sie die erforderlichen Angaben.

- Es können maximal 16 Communities eingestellt werden. Geben Sie die Community, ihre IP-Adresse, die SNMP-Version, Berechtigung und Zertifizierung ein.
- Löschen Sie die Eingaben in den Feldern [Community] und [IP address], um einen Eintrag zu entfernen.

Tabelle 5.4 Ein- und Ausgabe von Daten im Fenster [SNMP Community]

Feld	Beschreibung
<System Information>	
System Name	Enthält den PRIMEQUEST-Systemnamen, der im Fenster [System Information] eingegeben wird. Geben Sie den Namen im Fenster [System Information] ein (Abschnitt 2.2.4.3, „Systemnamen festlegen“).
System Location	Gibt den Standort des Systems an. Anm.: Folgende Zeichen könne verwendet werden: [0-9],[a-z],[A-Z], (n-Leerzeichen) ! " # $ % & ' ( ) = - ^ ~ \ @ ` [ ] { } : * ; + ? < . > , / _ | Es gelten folgende Einschränkungen: • Der String darf nicht mit einem der folgenden Zeichen beginnen: # (n-Leerzeichen) • Der String darf nicht mit einem der folgenden Zeichen enden: (n-Leerzeichen)
System Contact	Gibt die Kontaktperson für das System an. Anm.: Folgende Zeichen könne verwendet werden: [0-9],[a-z],[A-Z], (n-Leerzeichen) ! " # $ % & ' ( ) = - ^ ~ \ @ ` [ ] { } : * ; + ? < . > , / _ | Es gelten folgende Einschränkungen: • Der String darf nicht mit einem der folgenden Zeichen beginnen: # (n-Leerzeichen) • Der String darf nicht mit einem der folgenden Zeichen enden: (n-Leerzeichen)
<Community>	
Community	Gibt die SNMP-Community an. Anm.: Folgende Zeichen könne verwendet werden: [0-9],[a-z],[A-Z], (n-Leerzeichen) ! " # $ % & ' ( ) = - ^ ~ \ @ ` [ ] { } : * ; + ? < . > , / _ | Der String darf nicht mit einem der folgenden Zeichen beginnen: " ' ` #

Tabelle 5.4 Ein- und Ausgabe von Daten im Fenster [SNMP Community]

Feld	Beschreibung
IP Address/MASK	Gibt die IP-Adresse bzw. die Netzwerkadresse an. IP-Adresse und Subnetzmaske spezifizieren ein Subnetz wie folgt: <subnet-IP-address>/<number-of-subnet-mask-bits> Zum Beispiell wird durch die IP-Adresse 10.10.10.0 und die Subnetzmaske 255.255.255.0 das folgende Subnetz spezifiziert: 10.10.10.0/24
SNMP Version	Gibt die SNMP-Version (1, 2 oder 3) an.
Access	Legt die Zugriffsberechtigung fest. • [Read Only]: nur Leseberechtigung. • [Read Write]: Lese- und Schreibberechtigung.
Auth	Legt die verwendete Sicherheitsstufe fest. Dieses Feld steht nur zur Verfügung, wenn im Feld [SNMP Version] die Version 3 gewählt wurde. Wenn dort die Version 1 oder 2 ausgewählt wurde, erscheint in diesem Feld automatisch [noauth]. • noauth: Authentifizierung wird nicht verwendet. • auth: Authentifizierung wird verwendet. • priv: Authentifizierung und die Privacy-Funktion (Datenverschlüsselung) werden eingesetzt.

3 Klicken Sie auf [Apply], um die Eingaben zu übernehmen.

Ziel für SNMP-Traps einstellen

- Vorgehensweise

1 Wählen Sie [Network Configuration] → [SNMP Configuration] → [SNMP Trap]. Das Fenster [SNMP Trap] wird angezeigt.

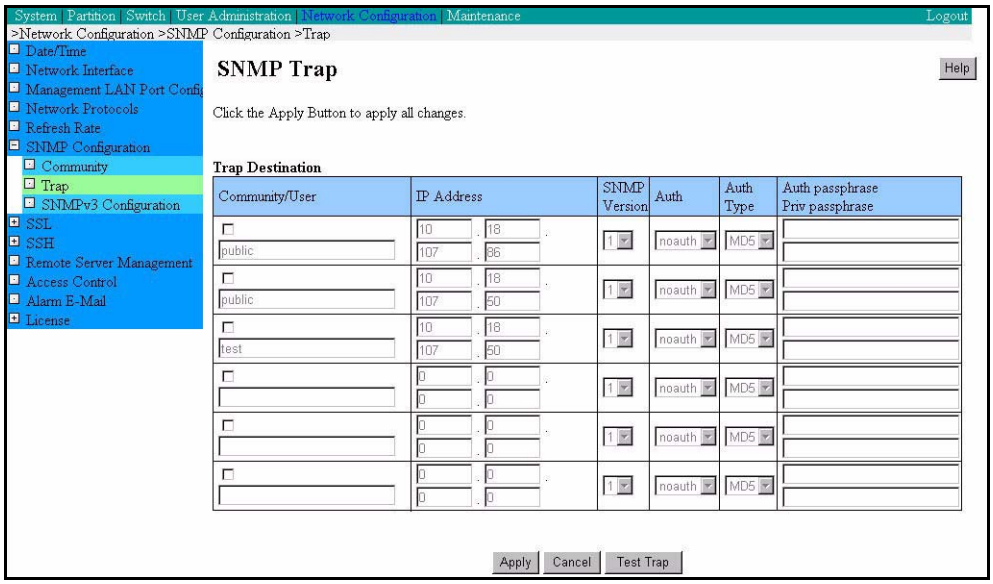


Abbildung 5.5 Das Fenster [SNMP Trap] (Beispiel)

2 Geben Sie ein Ziel für übertragene Traps an.

- Es können maximal 16 Trap-Ziele angegeben werden.
- Geben Sie eine Community bzw. einen Benutzername und die IP-Adresse des Zielrechners der Traps, die SNMP-Version und die Sicherheitsstufe an.

Tabelle 5.5 Ein- und Ausgabe von Daten im Fenster [SNMP Trap]

Feld	Beschreibung
Community/User	Name der Community bzw. des Benutzers. Anm.: Folgende Zeichen können benutzt werden: [0-9],[a-z],[A-Z], (n-Leerzeichen) ! " # $ % & ' ( ) = - ^ ~ \ @ ` [ ] { } : * ; + ? < . > , / _ | Der String darf nicht mit einem der folgenden Zeichen beginnen: " ' ` #
IP Address	IP-Adresse des Trap-Ziels.
SNMP Version	Auswahl der SNMP-Version. • 1: Eine SNMP-Trap der Version 1 wird übertragen • 2: Eine SNMP-Trap der Version 2 wird übertragen • 3: Eine SNMP-Trap der Version 3 wird übertragen

Tabelle 5.5 Ein- und Ausgabe von Daten im Fenster [SNMP Trap]

Feld	Beschreibung
Auth	Auswahl der Sicherheitsstufe. • noauth: Authentifizierung und Verschlüsselung auf der Basis eines Kennwortes deaktiviert (Authentifizierung auf der Basis eines Benutzernamens). • auth: Authentifizierung auf der Basis eines Kennwortes aktiviert, Verschlüsselung deaktiviert. • priv: Authentifizierung und Verschlüsselung auf der Basis eines Kennwortes aktiviert.
Auth Type	• md5: legt MD5 für Kennwort-basierte Verschlüsselung fest. • sha: legt SHA für Kennwort-basierte Verschlüsselung fest.
Auth passphras	Zeigt das Kennwort für die Paketverschlüsselung zum Zeitpunkt der Kennwort-basierten Authentifizierung an (keine Kennwort-basierte Verschlüsselung).
Priv passphrase	Zeigt das Kennwort für die Paketverschlüsselung zum Zeitpunkt der Kennwort-basierten Authentifizierung und Verschlüsselung an

3 Klicken Sie auf [Apply], um die Eingaben zu übernehmen.
Klicken Sie auf die Schaltfläche [Test Trap], um eine Test Trap an das aktuelle Trap-Ziel zu senden.

SNMP-V3 Einstellungen vornehmen

Mit dieser Funktion wird eine Engine-ID und ein Benutzer für SNMP V3 festgelegt.

Hinweis: Wird die Engine-ID oder die IP-Adresse geändert, müssen die Einstellungen für den Benutzer der SNMP Version 3 vollständig neu erfolgen. Der SNMP-Dämon muss kurz gestoppt und wieder gestartet werden, um den Benutzer zu überprüfen. Wenn also hier die Schaltfläche [Apply] geklickt wird, wird der SNMP-Dienst kurz angehalten.

- Vorgehensweise

1 Wählen Sie [Network Configuration] → [SNMP Configuration] → [SNMP v3 Configuration].
Das Fenster [SNMP v3 Configuration] wird angezeigt.

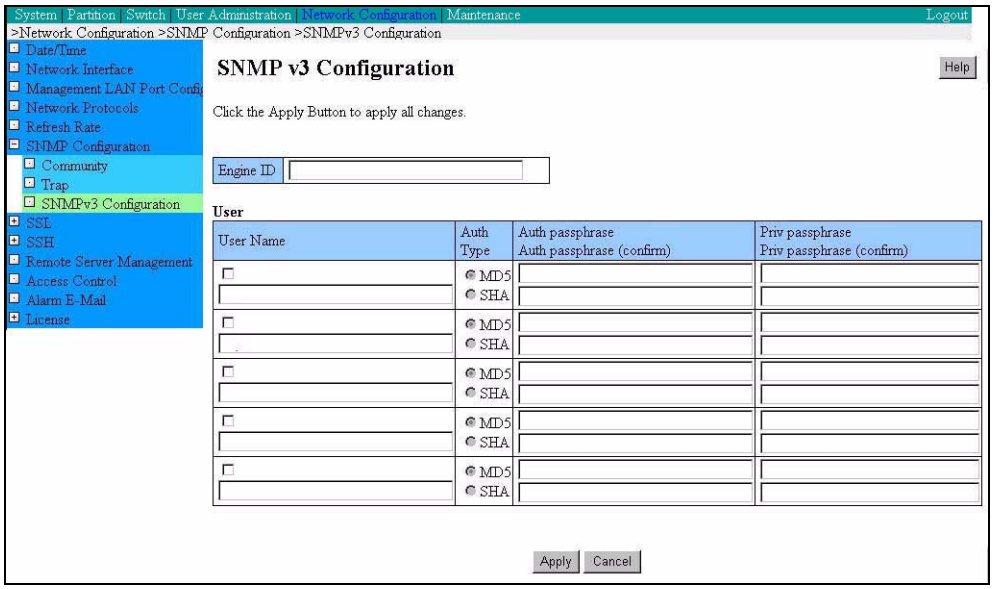


Abbildung 5.6 Das Fenster [SNMP v3 Configuration] (Beispiel)

2 Geben Sie einen SNMP Version 3 Benutzer ein.
Maximal 16 Benutzer können registriert werden.

Tabelle 5.6 Ein- und Ausgabe von Daten im Fenster [SNMP v3 Configuration]

Feld	Beschreibung
Engine ID	Engine-ID angeben. Anm.: Folgende Zeichen können benutzt werden: [0-9],[a-z],[A-Z], (n-Leerzeichen) ! " # $ % & ' ( ) = - ^ ~ \ @ ` [ ] { } : * ; + ? < . > , / _ | Es gelten folgende Einschränkungen: • Der String darf nicht mit einem der folgenden Zeichen beginnen: # (n-Leerzeichen) • Der String darf nicht mit einem der folgenden Zeichen enden: (n-Leerzeichen)
User	
User Name	Geben Sie den Benutzernamen ein. Aktivieren Sie das betreffende Kontrollkästchen, damit Sie den Namen des Empfängers in diesem Feld eingeben zu können. Remark: Folgende Zeichen können benutzt werden: [0-9],[a-z],[A-Z], (n-Leerzeichen) ! " # $ % & ' ( ) = - ^ ~ \ @ ` [ ] { } : * ; + ? < . > , / _ | Der String darf nicht mit einem der folgenden Zeichen beginnen: " ' ` #
Auth Type	Wählen Sie den Authentifizierungsmodus. • MD5: Kennwortverschlüsselung mit MD5. • SHA: Kennwortverschlüsselung mit SHA.
authpassphrase	Schlüsselwort für die Paketverschlüsselung bei Kennwort-Authentifizierung (keine Verschlüsselung).
privpassphrase	Schlüsselwort für die Paketverschlüsselung bei Kennwort-Authentifizierung und Verschlüsselung.

3 Klicken Sie auf [Apply], um die Eingaben zu übernehmen.
Starten Sie SNMP neu, damit die Einstellungen in Kraft treten.

5.1.3 SSH-Parameter festlegen

Legen Sie die SSH-Parameter für MMBs fest. Dazu sind Systemverwalterrechte erforderlich.

Vorgehensweise

1 Wählen Sie [Network Configuration] → [Network Protocols].
Das Fenster [Network Protocols] wird angezeigt.

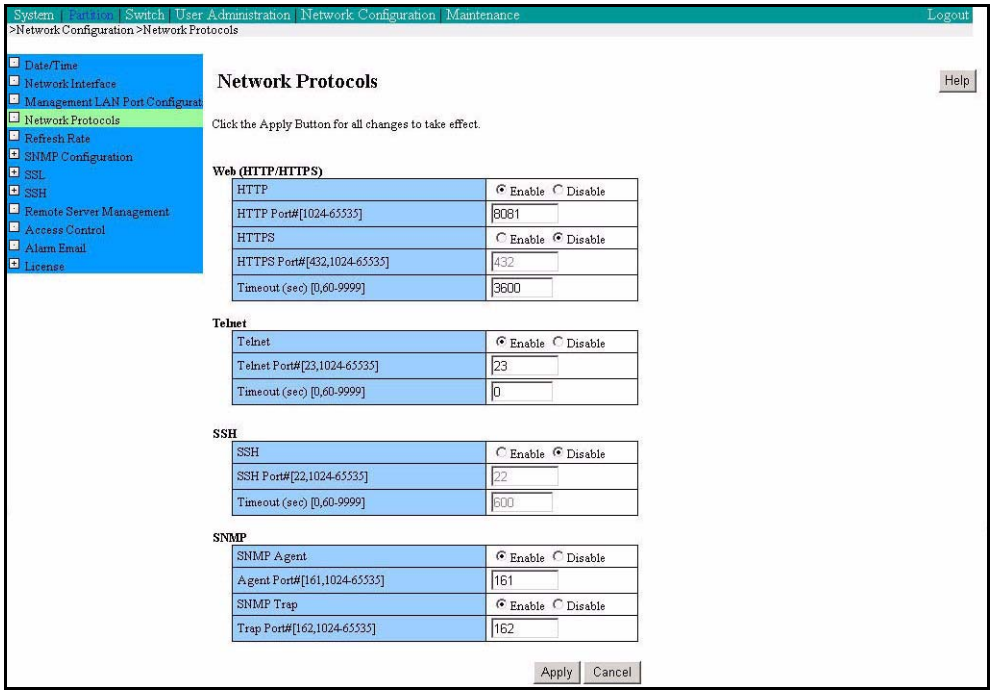


Abbildung 5.7 Das Fenster [Network Protocols] (Beispiel)

2 Nehmen Sie die für SSH erforderlichen Einstellungen vor.

Tabelle 5.7 Einstellungen für SSH

Feld	Beschreibung
<SSH>	
SSH	Aktiviert bzw. deaktiviert SSH. Voreinstellung: [Disable]
SSH Port	Legt den SSH-Port fest. Voreinstellung: 22
Timeout	Legt den Timeout-Wert für die Eingabe von Daten über SSH fest. Voreinstellung: 600 Sekunden

3 Klicken Sie auf [Apply], um die Eingaben zu übernehmen.

5.1.4 HTTPS-Parameter festlegen

Geben Sie die HTTPS-Parameter für MMB an. Dazu sind Systemverwalterrechte erforderlich.

Es ist ein gültiges SSL-Zertifikat erforderlich, um HTTPS aktivieren zu können. Wenn das Zertifikat nicht registriert ist, wird eine Fehlermeldung ausgegeben.

Wenn diese Einstellungen bereits vom Kundendienst-Techniker für die Ausführung des Testprogramms vorgenommen wurden, ist dieser Arbeitsschritt nicht mehr erforderlich.

Vorgehensweise

1 Wählen Sie [Network Configuration] → [Network Protocols].
Das Fenster [Network Protocols] wird angezeigt.

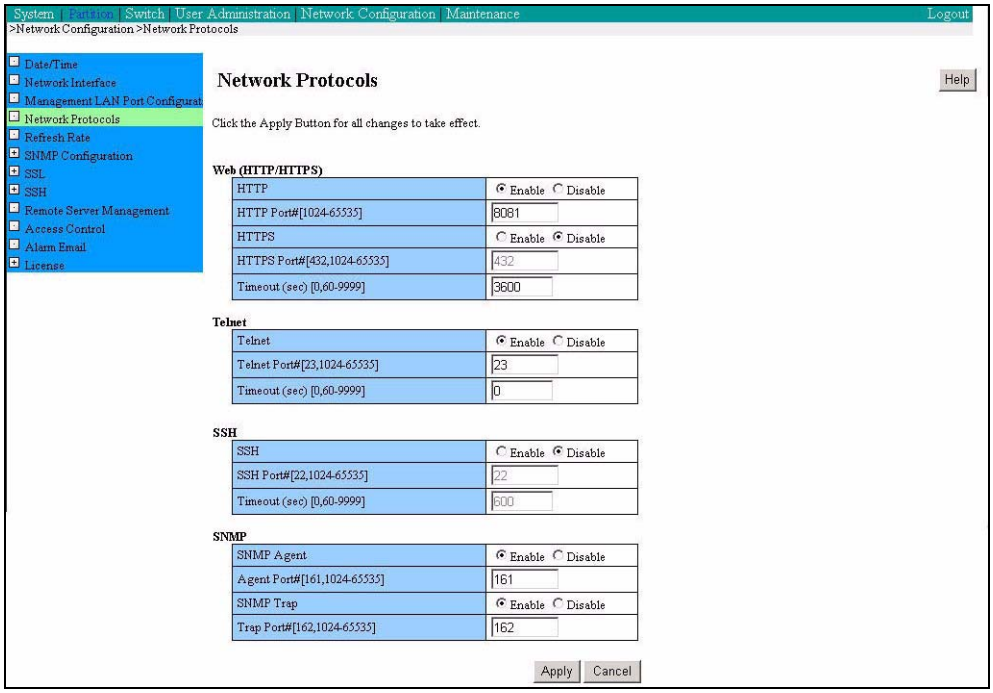


Abbildung 5.8 Das Fenster [Network Protocols] (Beispiel)

2 Führen Sie die für HTTPS erforderlichen Einstellungen unter [Web (HTTP/HTTPS)] durch.

Tabelle 5.8 Einstellungen für HTTPS

Feld	Beschreibung
<Web (HTTP/HTTPS)>	
HTTPS	Aktiviert bzw. deaktiviert HTTPS. Voreinstellung: [Disable]
HTTPS Port#	Legt die für HTTPS zu verwendende Portnummer fest. Voreinstellung: 432
HTTP/HTTPS Timeout	Legt den Timeout-Wert für den Empfang von Daten über HTTP/HTTPS fest. Voreinstellung: 600 Sekunden

3 Klicken Sie auf [Apply], um die Eingaben zu übernehmen.

KAPITEL 6 GSWB initialisieren

Wenn Sie das optionale Produkt GSWB in der PRIMEQUEST 580A/540A*/580/540/480/440 einsetzen wollen, müssen Sie es gemäß den Anweisungen im *PRIMEQUEST GSWB User's Manual* (U41635-J-Z816-x-76/C122-E028EN), initialisieren.

*: wird von Fujitsu Technology Solutions nicht unterstützt

Anhang A Zum Lieferumfang der PRIMEQUEST gehörende Software

In der folgenden Tabelle werden die Softwareprogramme aufgeführt, die zum Lieferumfang eines PRIMEQUEST-Systems gehören.
Y: wird unterstützt

Tabelle A.1 Liste der Software-Programme, die mit der PRIMEQUEST-Hardware geliefert werden

Nr.	Software	Funktion	EFI	Unterstützte Betriebssysteme		
				Linux (Red Hat)	Linux (SUSE)	Windows
1	EFI/BIOS	Firmware	Y	Y	Y	Y
2	PSA	Hardware-Verwaltung	-	Y	Y	Y
3	SIRMS	Konfigurationsdaten sammeln	-	Y*1	-	Y (*1)
SCSI						
4	Treiber	Treiber	Y	Y	Y	Y
5	Fusion MPT EFI	Firmware aktualisieren	Y	-	-	-
6	Fusion MPT Management Tool	CIMS-Browser	-	Y	Y	-
Broadcom-LAN						
7	Treiber	Treiber	-	Y	-	Y
8	BCM EFI		Y	-	-	-
9	BACS(Win)	VLAN, Aggregation usw.	-	-	-	Y
Intel-LAN						
10	Treiber	Treiber	-	Y	Y	Y
11	Intel PROSet(Win)	VLAN, AFT/ALB etc.	-	-	-	Y
Neterion-LAN						
12	Treiber	Treiber	-	Y	-	Y
13	Xframe Control Panel (Win)	VLAN, Team, etc.	-	-	-	Y
Emulex-FC						
14	Treiber	Treiber	Y	Y	Y	Y
15	lputil		-	Y	Y	Y
16	HBAnywhere		-	Y	Y	Y
Sonstige						
17	HBA-Blockiertreiber für PCL		-	Y	-	-

Tabelle A.1 Liste der Software-Programme, die mit der PRIMEQUEST-Hardware geliefert werden

Nr.	Software	Funktion	EFI	Unterstützte Betriebssysteme		
				Linux (Red Hat)	Linux (SUSE)	Windows
18	Log Trace Capture	Logdaten sammeln	-	Y (*1)	-	-
19	sadump (Standalone)	Dump erstellen	-	Y (*2)	-	-
20	Installation Support Tool	Auf externem Windows-PC ausführen, um die Datei ks.cfg zu erstellen.	-	Y	Y	-
21	Installation Support Tool für Windows	Tool zur Erzeugung einer Installationsdiskette für eine automatisierte Windows-Installation	-	-	-	Y
22	Bundled-Software Package Tool	Installationstool für Bundled Software	-	Y	Y	-
23	DSNAP	Sammelt mit Hilfe von BS-Kommandos BS-Basisinformationen	-	-	-	Y
24	PRIMEQUEST Software Installer	Zum Lieferumfang gehörende Software installieren	-	-	-	Y
25	System Parameter Check Tool	Überprüft die vom Benutzer gesetzten Umgebungsvari-ablen (für ein lauffähiges BS erforderliche Einstellun-gen).	-	Y	-	-
26	fjsnap (Sammelt System-informationen)	Sammelt mit Hilfe von BS-Kommandos vom Support benötigte Informationen	-	Y	Y	-
27	SystemcastWizard Lite	Remote-Installation Sicherung und Wiederherstellung	-	Y	Y	Y
28	SNMP MIB	MIB	-	Y	Y	Y
29	Software Support Guide	Sammelt mit Hilfe von BS-Kommandos vom Support benötigte Informationen	-	-	-	Y
30	HRM/server	Tool zur Unterstützung der Wartung	-	Y	-	Y

*1: Wird nur in Japan unterstützt.

*2: Wird nur in Japan und in der Region Asien unterstützt.

A.1 Software-Kategorien

Die PRIMEQUEST nutzt Software-Bundle-Packages. In diesem Kapitel erhalten Sie einen Überblick über diese Packages und die Installation und den Betrieb von SystemcastWizard Lite.

- Installation Support Tool (→ A.2)
- Bundled-Software Package Installer (→ A.3)
- DSNAP (→ A.4)
- System Parameter Check Tool (→ A.5)
- System Data Output Tool (fjsnap) (→ A.6)
- SystemcastWizard Lite (→ A.7)
- Installation Support Tool für Windows (→ A.8)
- Software Support Guide (→ A.9)

A.2 Installation Support Tool

Mit dem Installation Support Tool wird eine Konfigurationsdatei erstellt, die alle zur Installation des Linux-Betriebssystems erforderlichen Einstellungen enthält. Das Installation Support Tool kann mit der folgenden Betriebssystemversion eingesetzt werden:

- Red Hat Enterprise Linux AS (V.4 für Itanium)
- Red Hat Enterprise Linux 5 (für Intel Itanium)
- SUSE Linux Enterprise Server 9 for Itanium Processor Family
- SUSE Linux Enterprise Server 10 for Itanium Processor Family

Das Betriebssystem wird auf der PRIMEQUEST so installiert, wie es in der Konfigurationsdatei zuvor mit Hilfe des Installation Support Tools auf einem Windows-PC konfiguriert wurde, um die die Betriebssysteminstallation zu bewerkstelligen.

Der Bundled-Software Package Installer erleichtert die Installation der mitgelieferten Software.

Näheres finden Sie im *PRIMEQUEST Installation Support Tool User's Guide (Red Hat)* (C122-E005EN) und im *PRIMEQUEST Installation Support Tool User's Guide (SUSE)* (C122-E047EN).

A.3 Bundled-Software Package Installer

Mit dem Bundled-Software Package Installer werden die von der PRIMEQUEST benötigten Utilities installiert.

Der Bundled-Software Package Installer kann mit folgenden Betriebssystem-Versionen eingesetzt werden:

- Red Hat Enterprise Linux AS (V.4 für Itanium)
- Red Hat Enterprise Linux 5 (für Intel Itanium)
- SUSE Enterprise Linux (Server 10 for Itanium Processor Family)

Näheres finden Sie im *PRIMEQUEST Bundled-Software Package Installer User's Guide* (C122-E006EN).

A.4 DSNAP

DSNAP sammelt Diagnosedaten, wenn in einem Windows-Betriebssystem ein Problem auftritt. Der Kundendienst-Techniker verwendet dieses Werkzeug, um Angaben zur Systemkonfiguration zu sammeln, mit deren Hilfe er die Ursache des aufgetretenen Problems ermittelt.

- Installation

Näheres finden Sie in Abschnitt 3.3.6, „High Reliability Tools“.

- Nutzung

Lesen Sie die Datei \DSNAP README.TXT.

A.5 System Parameter Check Tool

Einige Systemeinstellungen, die mit großer Wahrscheinlichkeit im Linux-Kernel geändert werden, können einen normalen Betrieb des Linux-Systems stören. Das System Parameter Check Tool erkennt und meldet derartige Einstellungen. Das System Parameter Check Tool kann mit der folgenden Betriebssystemversion eingesetzt werden:

- Red Hat Enterprise Linux AS (V.4 für Itanium)
- Red Hat Enterprise Linux 5 (für Intel Itanium)

Das System Parameter Check Tool enthält Kommandos, die Systemparameter überprüfen und einstellen sowie eine Funktion, die automatische Überprüfungen beim Hoch- und Herunterfahren des Systems durchführt.

Der Einsatz des System Parameter Check Tools verhindert Fehler beim Hochfahren des Systems, die durch fehlerhafte Einstellungen verursacht werden. Ferner überprüft es die Größe des Dump-Bereichs.

Näheres finden Sie im *PRIMEQUEST System Parameter Check Tool User's Guide* (C122-E009EN).

A.6 System Data Output Tool (fjsnap)

fjsnap sammelt Diagnosedaten, die für die Fehlerbehebung benötigt werden.

fjsnap sammelt aus über 1.000 Dateien Informationen über Hardware- und Software-Konfiguration, Umgebungseinstellungen, Betriebs- und Loginformationen, die für die Fehlerdiagnose und -behebung benötigt werden und komprimiert diese Informationen in einer einzigen Datei.

Die folgende Abbildung bietet einen Überblick über die von fjsnap gesammelten Systeminformationen:

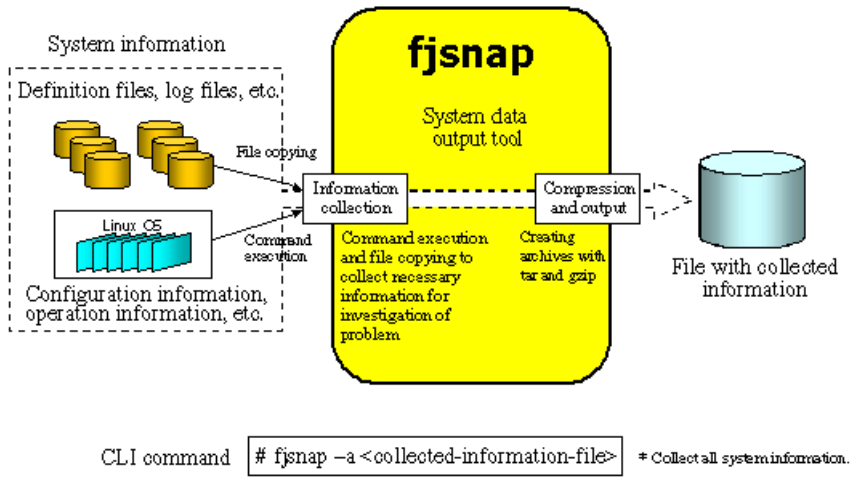


Abbildung A.1 Sammeln von Systemdaten mit fjsnap

Weitere Informationen über fjsnap finden Sie im *PRIMEQUEST 500A/500/400 Series Reference Manual: Messages/Logs* (U41634-J-Z816-x-76/C122-E004EN).

A.7 SystemcastWizard Lite

A.7.1 SystemcastWizard Lite im Überblick

Mit SystemcastWizard Lite kann über ein Netzwerk ein Betriebssystem installiert oder eine Datensicherung bzw. Wiederherstellung durchgeführt werden, wodurch der erforderliche Arbeitsaufwand bei der Installation mehrerer Partitionen erheblich reduziert werden kann. Der Benutzer wird Schritt für Schritt am Bildschirm durch die erforderlichen Arbeitsschritte geleitet, ohne CD-ROMs oder sonstige Medien einlegen zu müssen.

Entfernte Installation eines Betriebssystems

Bei einer Remote-Installation wird ein neues Betriebssystem über das Netzwerk installiert. Sämtliche Installationsprozesse werden automatisch auf der Grundlage zuvor festgelegter Einstellungen durchgeführt. Der erforderliche Arbeitsaufwand kann deutlich verringert werden, da dieselbe Konfiguration gleichzeitig in beliebig vielen Partitionen installiert werden kann.

Sicherung/Wiederherstellung

Systemdatenträger können mit SystemcastWizard Lite über das Netzwerk gesichert bzw. wiederhergestellt werden. Da immer nur die Daten jeweils eines Laufwerks gesichert bzw. wiederhergestellt werden, ist diese Funktion sehr hilfreich, um das System während der Einrichtung oder Überprüfung zu sichern bzw. nach einem Systemausfall wiederherzustellen. Die Netzwerkaktivierung erleichtert die Wiederherstellung des Systemdatenträgers, wenn das Betriebssystem nicht aktiv ist.

A.7.2 SystemcastWizard Lite konfigurieren

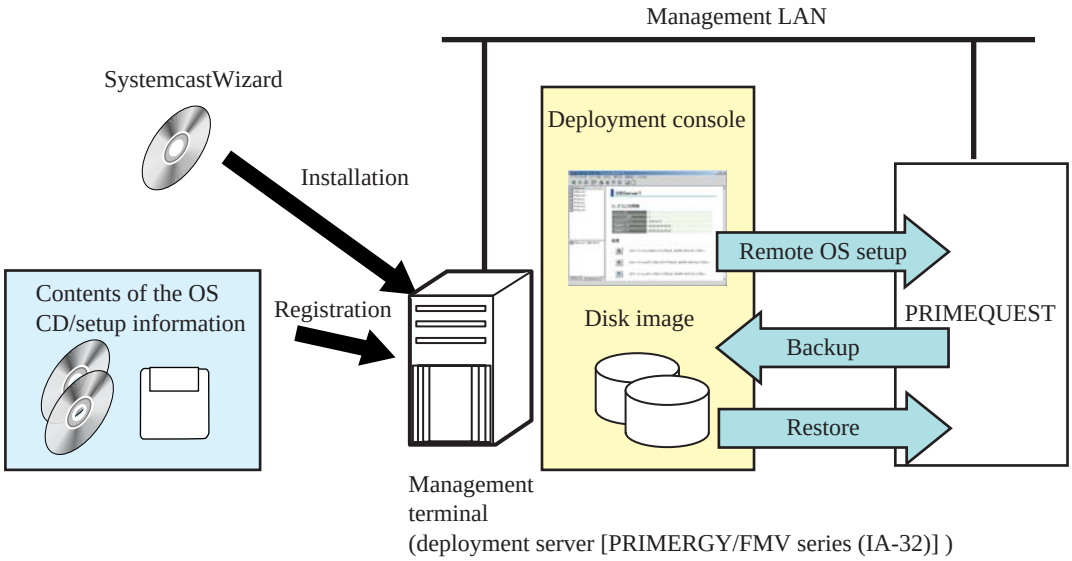


Abbildung A.2 Konfiguration der Bundled-Version von SystemcastWizard Lite

Installieren Sie SystemcastWizard Lite auf einem an das Management-LAN angeschlossenen Rechner und richten Sie ein Management-Terminal (Installationsserver) ein. Von der Management-Konsole (Installationskonsole) dieses Terminals aus kann eine entfernte Installation bzw. Sicherung/Wiederherstellung des Betriebssystems der PRIMEQUEST durchgeführt werden.

Beachten Sie, dass DHCP (*1) über das Netzwerk gestartet wird. Beachten Sie ferner, dass ein FTP-Server für die entfernte Einrichtung von Linux erforderlich ist.

*1 SystemcastWizard Lite enthält einen einfachen DHCP-Server.

A.7.3 SystemcastWizard Lite installieren

Zunächst müssen Sie den SystemcastWizard Lite installieren.

Installieren Sie SystemcastWizard Lite indem Sie die setup.exe ausführen, die sich auf der zum Lieferumfang Ihrer PRIMEQUEST gehörenden PRIMEQUEST „SystemcastWizard Lite“ CD-ROM befindet. Folgen Sie den Anweisungen des Installers.

Weitere Angaben finden Sie im Handbuch *PRIMEQUEST SystemcastWizard Lite User's Guide* (C122-E010EN).

A.7.4 SystemcastWizard Lite benutzen

Wählen Sie im Start-Menü des Management-Terminals, auf dem Sie SystemcastWizard Lite installiert haben, [Programs] - [SystemcastWizard Lite] - [Deployment Console]. Die Installationskonsole wird gestartet.

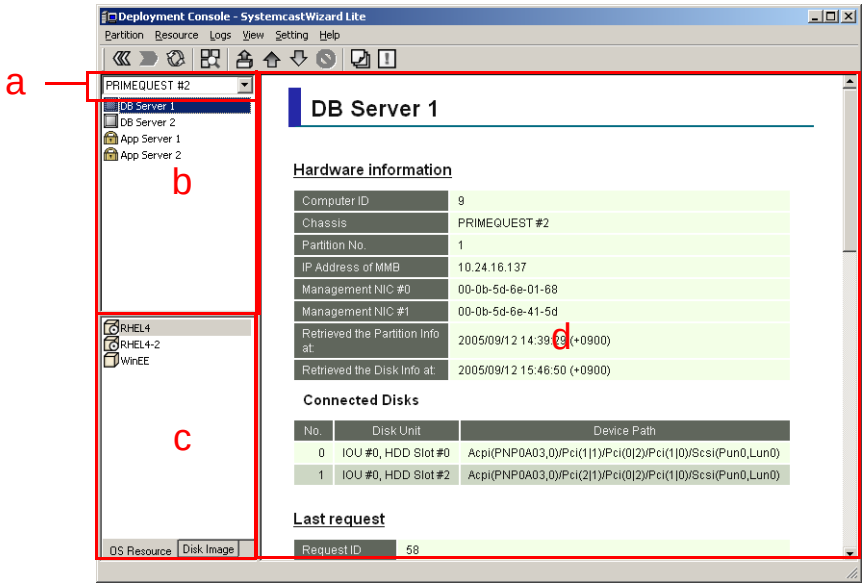


Abbildung A.3 Installationskonsole starten

Bestandteile des Fensters

Die Installationskonsole ist in folgende Bereiche untergliedert:

a Schrankname (Dropdown-Liste)
Wenn mehrere Schränke registriert sind, können Sie aus dieser Liste den gewünschten Schrank auswählen.

b Partitionen
Zeigt eine Liste der in dem ausgewählten Schrank enthaltenen Partitionen an.

c Ressourcen
Zeigt eine Liste der Ressourcen und Plattenimages an.

d Detailansicht
Zeigt Informationen über die ausgewählte Partition, Ressource, Logdatei, usw. an.

Arbeitsablauf

Der Arbeitsablauf sieht wie folgt aus:

1 Wählen Sie im oberen linken Teilfenster eine Ziel-Partition aus.

2 Wählen Sie im Menü die Aufgabe aus, die Sie durchführen wollen (Installation des Betriebssystems, Sicherung/Wiederherstellung). Ein Dialogfeld wird geöffnet.

3 Folgen Sie den im Dialogfeld gegebenen Anweisungen, um die Software zu installieren und in Betrieb zu nehmen.
Im rechten Teilfenster, der Detailansicht, können Sie den Fortschritt der Installation verfolgen.

Weitere Informationen finden Sie im *PRIMEQUEST SystemcastWizard Lite User's Guide* (C122-E010EN).

A.7.5 Zur Beachtung

Nur SystemcastWizard Lite, das mit der Systemeinheit ausgeliefert wird, kann bei PRIMEQUEST-Geräten eingesetzt werden.

A.8 Installation Support Tool für Windows

Das Installation Support Tool für Windows ist ein Tool zur automatisierten Installation von Windows auf einem PRIMEQUEST-System.

Einzelheiten finden Sie im *PRIMEQUEST Installation Support Tool for Windows User's Guide* (C122-048EN).

Das *PRIMEQUEST Installation Support Tool for Windows User's Guide* (C122-048EN) finden Sie in folgendem Verzeichnis auf der „PRIMEQUEST Drivers CD for Microsoft® Windows Server® 2003“ (C122-E024):

E:\Tools\General\IST\manual (wenn E das CD-ROM-Laufwerk ist)

A.9 Software Support Guide

Beim Software Support Guide handelt es sich um eine Gruppe von Programmen, die zusammen Informationen über Windows-Software-Probleme sammeln und geordnet aufzeichnen.

Kundendienst-Techniker werten diese Informationen aus und könne den Systemzustand beim Auftreten von Fehlern diagnostizieren und die Fehlerursachen herausfinden.

Die folgende Tabelle zeigt die Tools des Software Support Guide, die die Fehlerbehebung unterstützen.

Tabelle A.2 Informationen, die die Tools des Software Support Guide liefern

Name	Informationen
QSS (Quick Support System)	Registries, Event Logs, System File List, Watson Log, Minidumps und MSCS Cluster Log
User Mode Process Dumper	Application (Snapshot) Dump
Desktop Heap Monitor	Informationen über die Größe des Desktop Heap, einer Systemressource
ETW (Event Trace for Windows)	Standard-Trace-Funktion des Betriebssystems Es können getraced werden: Process/Thread, Festplatte und Netzwerk (ETW muss nach Installation des Software Support Guide gestartet werden.)

Einzelheiten finden Sie in der Online-Dokumentation des Software Support Guide.

Anhang B Installation

In diesem Anhang wird die Vorgehensweise bei der Installation einer PRIMEQUEST beschrieben. Die Installation umfasst folgende Maßnahmen:

- Anschluss eines PCs
- Initialisierung des MMB
- Anmeldung in der Web-UI

B.1 Anschluss eines PCs

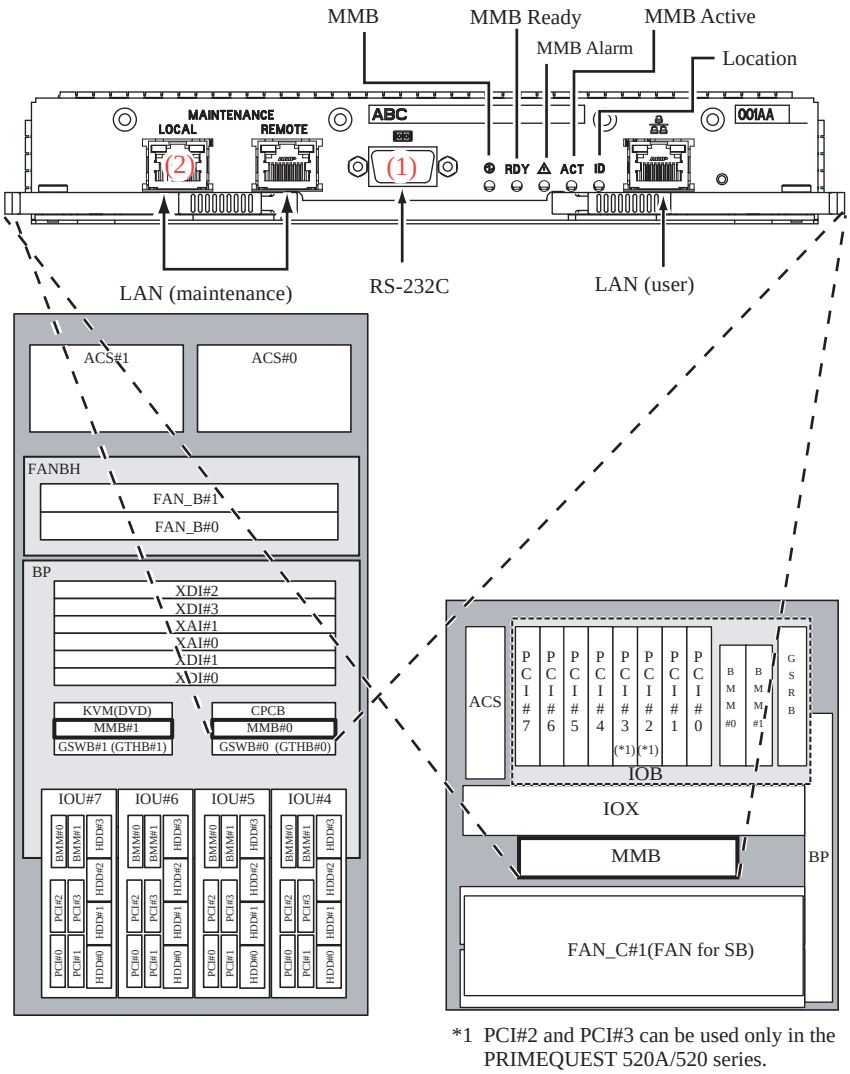
In diesen Abschnitt wird beschrieben, wie ein PC an die PRIMEQUEST Systemeinheit angeschlossen wird.

1 Verbinden Sie den COM-Port des PCs unter Verwendung eines RS-232C-Verbindungskabels mit der externen RS-232C-Schnittstelle des MMBs ((1) in Abbildung B.4).

2 Verbinden Sie den LAN-Port des PCs unter Verwendung eines LAN-Kabels mit der externen LAN-Schnittstelle des MMBs ((2) in Abbildung B.4).

Bem.: BMM#1 wird ausschließlich in der PRIMEQUEST 500A*/500-Modellreihe unterstützt.

*: wird von Fujitsu Technology Solutions nicht unterstützt



*1 PCI#2 and PCI#3 can be used only in the PRIMEQUEST 520A/520 series.

Rear view (PRIMEQUEST 580A/540A*/ 580/540/480/440)

Rear view (PRIMEQUEST 520A*/520/420)

*: not supported by Fujitsu Technology Solutions

Abbildung B.4 Position des MMBs und der externen Schnittstellen

Tabelle B.3 Externe Schnittstellen des MMBs

Externe Schnittstelle		Anzahl	Bemerkung
RS-232C		1	Wird vom Kundendienst-Techniker für das Einrichten der Systemeinheit benutzt. Wird im Normalbetrieb nicht benutzt.
LAN	100Base-TX	3	• LAN (Benutzer): Konsolenanschluss • Maintenance: [LOCAL]: ausschließliche Verwendung durch Kundendienst-Techniker [REMOTE]: REMCS*-Port

*: wird von Fujitsu Technology Solutions nicht unterstützt

3 Schalten Sie den PC ein und starten Sie die Terminalsoftware.
Führen Sie die folgenden Einstellungen durch.

Tabelle B.4 Einstellungen der Terminalsoftware

Einstellung	Wert
Bits pro Sekunde	19.200
Datenbits	8
Parität	keine
Stopbit	1
Fluss-Kontrolle	nicht anwendbar
Emulation	VT100

B.2 MMB initialisieren

In diesem Abschnitt wird die Vorgehensweise bei der Initialisierung des MMB beschrieben.

1 Bringen Sie den Schalter MAIN LINE SWITCH in die Position ON, um das MMB einzuschalten.

2 Die ALM LED jeder Einheit leuchtet auf und die Ready-LED des MMBs blinkt (Initialisierung erfolgt). Warten Sie bis die ALM LED jeder Einheit nicht mehr leuchtet und die Ready-LED des MMBs konstant leuchtet (Initialisierung abgeschlossen).

3 Die Anmeldeaufforderung erscheint. Geben Sie „Administrator“ ein.

4 Sie werden nun aufgefordert, das Kennwort zu ändern. Geben Sie ein neues Kennwort ein.

Hinweis: Das Kennwort muss mindestens acht Zeichen lang sein und sollte so gewählt werden, dass es nicht leicht nachvollziehbar ist. Wenn das eingegebene Kennwort vom System nicht akzeptiert wird, werden Sie aufgefordert, ein anderes zu wählen.

5 Richten Sie das MMB-Netzwerk ein.
Legen Sie mithilfe des folgenden Kommandos die IP-Adresse fest:

```
Administrator> set ip <IP Address> <netmask>
Administrator> set gateway <defaut gateway IP Address>
```

Beispiel: 192.168.0.10 für die IP-Adresse, 255.255.255.0 für die Netzmaske und 192.168.0.1 für das Gateway

```
Administrator> set ip 192.168.0.10 255.255.255.0
Administrator> set gateway 192.168.0.1
```

6 Aktivieren Sie http, indem Sie das Kommando „set http enable“ ausführen.
Somit kann der Benutzer von einem PC aus über das LAN auf das MMB Web-UI zugreifen.

```
Administrator> set http enable
```

7 Aktivieren Sie telnet, indem Sie das Kommando „set telnet enable“ ausführen.

```
Administrator> set telnet enable
```

8 Stellen Sie das Systemdatum und die Uhrzeit ein.

```
Administrator> set date MMDDhhmm[[CC]YY][,ss]
```

Beispiel: Uhrzeit 13:10:00 und Datum April 27, 2005

```
Administrator> set date 04271310[[20]05][,00]
```

B.3 Anmelden beim Web-UI

In diesem Abschnitt wird beschrieben, wie Sie sich beim MMB Web-UI anmelden. Das MMB Web-UI unterstützt die folgenden Browser:

Internet Explorer: Version 5.5 (Service Pack2) oder höher
Netscape: Version 7.02 oder höher

Anm.:

- Da das MMB Web-UI JavaScript verwendet, muss JavaScript in den Einstellungen des Browsers auf dem verwendeten PC zugelassen sein.
- Da das MMB Web-UI Daten herunterlädt, muss das Herunterladen in den Einstellungen des Browsers auf dem verwendeten PC zugelassen sein.

1 Starten Sie den Browser und geben Sie die folgende URL ein:
http://<knotenname>:<adminport>
knotenname: IP-Adresse des MMB
adminport: die Nummer des Managementports des MMBs (Voreinstellung: 8081)
Beispiel: Die IP-Adresse ist 192.168.0.10.
http://192.168.0.10:8081

2 Die Web-UI des Managementboards wird angezeigt.

3 Melden Sie sich mit „Administrator“ an.

Das folgende Fenster wird angezeigt:

Username: Administrator

Password: Kennwort, das gemäß Section B.2, „MMB initialisieren“ eingegeben wurde.

Anm.: Web-UI-Fenster schließen

Klicken Sie in der Navigationsleiste (in der Abb. unten mit e) bezeichnet) auf [Logout], um das Web-UI-Fenster zu schließen.

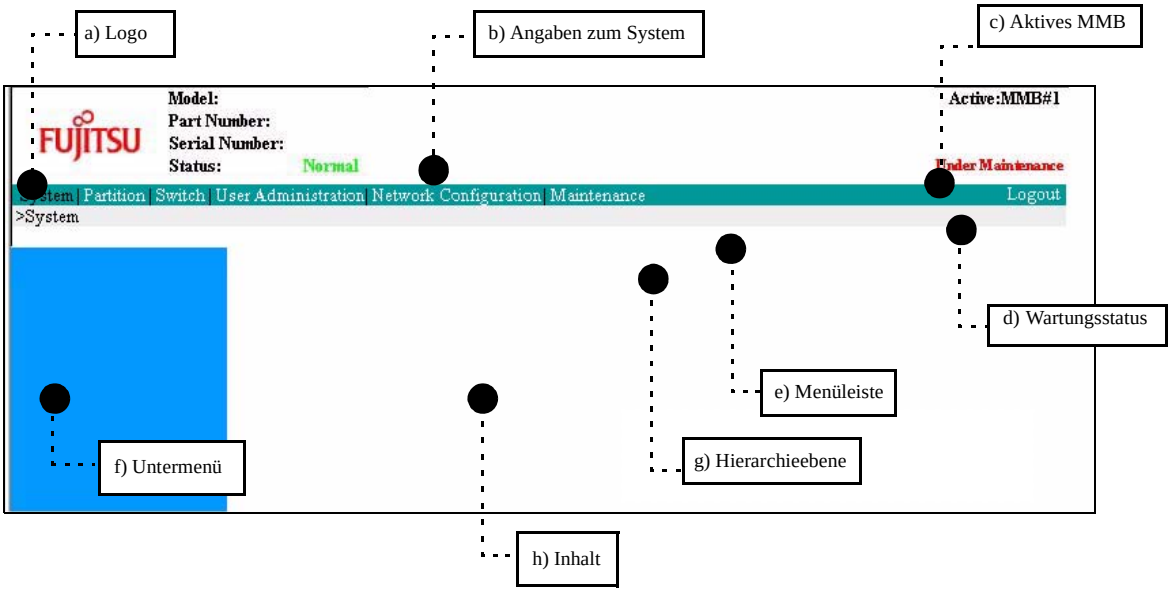


Abbildung B.5 Das Fenster [Web-UI Frame Information]

Anhang C Ein- und Ausschalten

Dieser Anhang beschreibt die Vorgehensweise beim Ein- und Ausschalten des Systems.

- Ein- und Ausschalten der Systemeinheit (→ C.1)
- Schränke und Partitionen ein- und ausschalten (→ C.2)
- Partitionen ein- und ausschalten (→ C.3)

C.1 Ein- und Ausschalten der Systemeinheit

Dieser Abschnitt beschreibt die folgenden Ein-/Ausschaltvorgänge für die Systemeinheit:

- Betätigung der Schutzschalter (→ C.1.1)
- Ein- und Ausschalten des gesamten Systems (→ C.1.2)

C.1.1 Betätigung der Schutzschalter

Dieser Abschnitt beschreibt, wie das System über den Schutzschalter ein- und ausgeschaltet wird.

Die Schutzschalter der PRIMEQUEST 580A/540A*/580/540/480/440 sind die Hauptschalter der Systemeinheit und schützen diese auch vor Überstrom.

Hinweis: FAN_E#0 und FAN_E#1 der PRIMEQUEST 520A*/520/420-Systeme arbeiten nicht nur beim Systembetrieb, sondern auch im Standby der Systeme.

- Einschalten des Systems über die Schutzschalter (PRIMEQUEST 580A/540A/580/540/480/440) (→ C.1.1.1)
- System einschalten (PRIMEQUEST 520A/520/420) (→ C.1.1.2)
- System über die Schutzschalter ausschalten (PRIMEQUEST 580A/540A/580/480/480/440) (→ C.1.1.3)
- System ausschalten (PRIMEQUEST 520A/520/420) (→ C.1.1.4)

---

*: wird von Fujitsu Technology Solutions nicht unterstützt

C.1.1.1 Einschalten des Systems über die Schutzschalter (PRIMEQUEST 580A/540A/580/540/480/440)

Hinweis zum Einschalten des Systems

Betätigen Sie zuerst die Schutzschalter im Basisschrank.

Wenn nicht alle Schutzschalter eingeschaltet sind, startet das System möglicherweise nicht ordnungsgemäß, da es nicht ausreichend mit Strom versorgt wird. Schalten Sie alle Schutzschalter in möglichst rascher Folge ein.

Anm.: Nach dem Ausschalten eines Schutzschalters müssen Sie mindestens 10 sekunden warten, bevor Sie den Schalter wieder einschalten.

In der Systemeinheit liegt ein Problem wie z. B. ein Kurzschluss vor, wenn der Schutzschalter wegen Überstrom abgeschaltet hat. Falls der schutzschalter dann wieder eingeschaltet wird, kann die Überstromsicherung im Anschlussschrank ausschalten, die Systemeinheit kann möglicherweise ausbrennen etc. Um solche Probleme zu verhindern, schalten Sie den Schutzschalter nicht wieder ein, und ziehen Sie einen Kundendienst-Techniker hinzu.

Einschalten

1 Schalten Sie die Schutzschalter an der Systemeinheit ein.
Öffnen Sie die Rückseite des Basisschranks und schalten Sie sämtliche Schutzschalter, oben im Schrank, in die Stellung „|“.

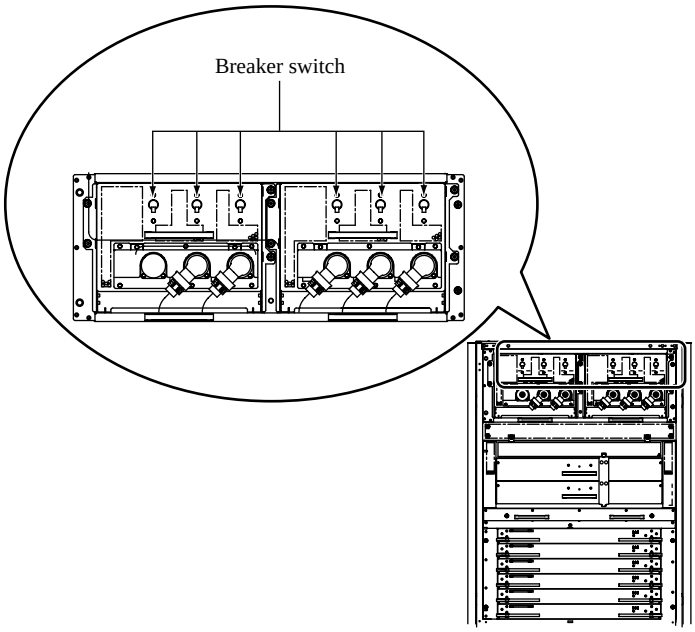


Abbildung C.1 Position der Schutzschalter (Basisschrank)

Hinweis: Die Anzahl der Schutzschalter hängt von der Art der Stromversorgung der Systemeinheit ab.
Abbildung C.2 zeigt eine PRIMEQUEST 580A/540A/580/480 mit Extended Power Cabinet.

2 Wenn die PRIMEQUEST 580A/540A/580/480 mit Extended Power Cabinet betrieben wird, schalten Sie alle Schutzschalter im Extended Power Cabinet ein. Öffnen Sie die Rückseite des Extended Power Cabinets und bringen Sie alle Schutzschalter in die Stellung „|“.

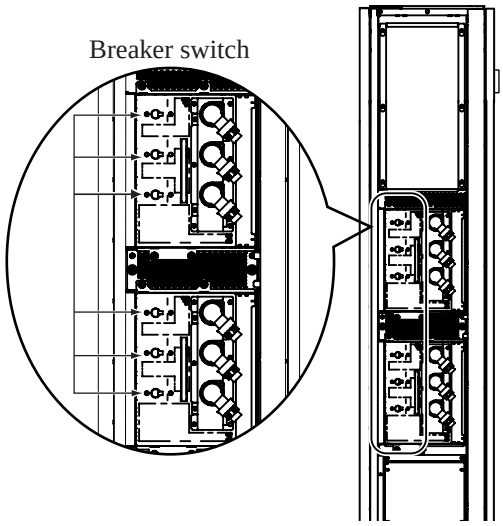


Abbildung C.2 Position der Schutzschalter (Extended Power Cabinet)

Hinweis: Die Anzahl der Schalter hängt von der Systemkonfiguration ab.
Abbildung C.2 zeigt ein Extended Power Cabinet, in den ein PSU (Netzteilerweiterungssatz) installiert ist.

3 Schalten Sie auch die Schutzschalter des Extended I/O Cabinets ein, wenn ein solcher angeschlossen ist.
Öffnen Sie die Tür an der Vorderseite des Extended I/O Cabinets und bringen Sie alle Schalter im Power Distribution Box (Netzverteiler) in die Stellung „1“.

Anm.: Die Art der im Extended I/O Cabinet installierten Power Distribution Box und Schutzschalter hängt von der Region ab, in der der Schrank eingesetzt wird.
Insbesondere in Europa werden in der Power Distribution Box des Extended I/O Cabinets keine Schutzschalter verwendet. Schalten Sie in diesem Fall die Schutzschalter auf dem Power Distribution Board (Netzverteilerboard) ein, mit dem die Stromversorgung des Extended I/O Cabinets verbunden ist.

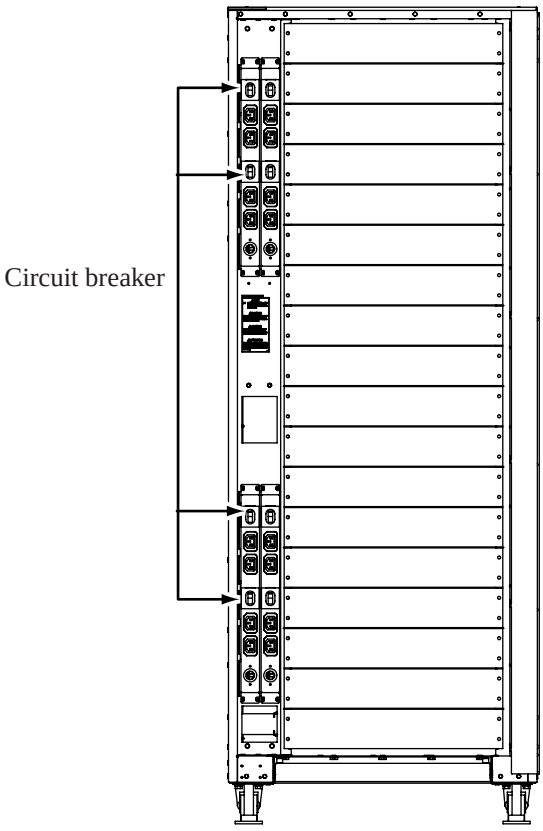


Abbildung C.3 Position der Schutzschalter (Extended I/O Cabinet)

C.1.1.2 System einschalten (PRIMEQUEST 520A*/520/420)

Anm.: Nach dem Ausschalten eines Schutzschalters müssen Sie mindestens 10 Sekunden warten, bevor Sie den Schalter wieder einschalten.

In der Systemeinheit liegt ein Problem wie z. B. ein Kurzschluss vor, wenn der Schutzschalter wegen Überstrom abgeschaltet hat. Falls der Schutzschalter dann wieder eingeschaltet wird, kann die Überstromsicherung im Anschlussschrank ausschalten, die Systemeinheit kann möglicherweise ausbrennen etc. Um solche Probleme zu verhindern, schalten Sie den Schutzschalter nicht wieder ein, und ziehen Sie einen Kundendienst-Techniker hinzu.

Einschalten

1 Schließen Sie das Kabel zuerst an das ACS der Systemeinheit und dann an die Power Distribution Box an.

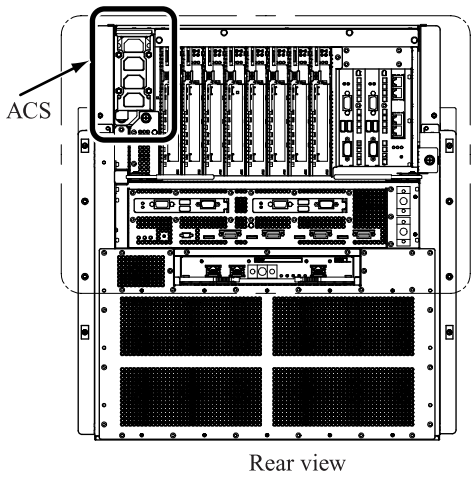


Abbildung C.4 Position des ACS

*: wird von Fujitsu Technology Solutions nicht unterstützt

C.1.1.3 System über die Schutzschalter ausschalten (PRIMEQUEST 580A/540A*/580/480/480/440)

Ausschalten

ACHTUNG

Datenverlust

Wenn das System vom MMB aus heruntergefahren wird, leuchten nur die folgenden LEDs des Bedienfeldes und des MMBs:

- MMB-Ready des Bedienfelds
- Power-LED des MMB
- Ready-LED des MMB
- Active-LED des MMB

Stellen Sie sicher, dass alle anderen LEDs aus sind (nur die oben aufgeführten LEDs dürfen noch leuchten), bevor Sie die Stromzufuhr zum System ausschalten (USV, Power Distribution Box, Hauptschalter).
Wenn das nicht der Fall ist, kann es zu Datenverlusten kommen.

1 Schalten Sie die Systemeinheit aus.
Verwenden Sie dazu das MMB (Management Board). Näheres finden Sie im Abschnitt C.1.2, „Ein- und Ausschalten des gesamten Systems“.

2 Vergewissern Sie sich, dass auf dem Bedienfeld und dem MMB nur noch die folgenden LEDs leuchten:
   - MMB-Ready LED des Bedienfeldes
   - Power-LED des MMB
   - Ready-LED des MMB
   - Active-LED des MMB

3 Wenn ein Extended Power Cabinet an die PRIMEQUEST 580A/540A*/580/480 angeschlossen ist, schalten Sie dort die Schutzschalter aus.
Öffnen Sie die Tür an der Rückseite des Extended Power Cabinet und bringen Sie sämtliche Schalter in die Stellung „0“.
   Anm.: Die Anzahl der Schutzschalter hängt von der Systemkonfiguration ab. (Siehe Abbildung C.2)
   Abbildung C.2 zeigt eine PRIMEQUEST 580A/540A*/580/480 mit installierter PSU.

*: wird von Fujitsu Technology Solutions nicht unterstützt

4 Schalten Sie die Schutzschalter der Systemeinheit aus.
Öffnen Sie die rückwärtige Tür der Systemeinheit und bringen Sie sämtliche Schutzschalter oben im Schrank in die Stellung „0“.
Hinweis: Die Anzahl der Schalter hängt von der Konfiguration der Einheit ab. (Siehe Abbildung C.2)
Abbildung C.2 zeigt eine PRIMEQUEST 580A/540A*/580/480 mit installierter PSU.

5 Schalten Sie die Schutzschalter des Extended I/O Cabinets aus, wenn ein solches angeschlossen ist.
Öffnen Sie die Vorderseite des Extended I/O Cabinets und bringen Sie sämtliche Schutzschalter der Power Distribution Box in die Stellung „0“.
Hinweis: Die Art der im Extended I/O Cabinet installierten Power Distribution Box und Schutzschalter ist abhängig von der Region, in der das System zum Einsatz kommt. (Siehe Abbildung C.3)
Insbesondere in Europa kommen in der Power Distribution Box im Extended I/O Cabinet keine Schutzschalter zum Einsatz. Schalten Sie in dem Fall die Schutzschalter auf dem Power Distribution Board aus, an das die Stromversorgung des Extended I/O Cabinets angeschlossen ist.

C.1.1.4 System ausschalten (PRIMEQUEST 520A*/520/420)

Ausschalten

⚠ ACHTUNG

Datenverlust

Wenn das System vom MMB aus heruntergefahren wird, dürfen nur die folgenden LEDs des Bedienfeldes und des MMBs noch leuchten:

- MMB-Ready des Bedienfelds
- Power-LED des MMB
- Ready-LED des MMB
- Active-LED des MMB

Stellen Sie sicher, dass alle anderen LEDs aus sind (nur die oben aufgeführten LEDs dürfen noch leuchten), bevor Sie die Stromzufuhr zum System ausschalten (USV, Power Distribution Box, Hauptschalter).
Wenn das nicht der Fall ist, kann es zu Datenverlusten kommen.

1 Schalten Sie die Systemeinheit aus.
Verwenden Sie dazu das MMB (Management Board). Näheres finden Sie im Abschnitt C.1.2, „Ein- und Ausschalten des gesamten Systems“.

*: wird von Fujitsu Technology Solutions nicht unterstützt

2 Vergewissern Sie sich, dass auf dem Bedienfeld und dem MMB nur noch die folgenden LEDs leuchten:
   - MMB-Ready LED des Bedienfeldes
   - Power-LED des MMB
   - Ready-LED des MMB
   - Active-LED des MMB

3 Ziehen Sie das Netzkabel von der Power Distribution Box ab.

C.1.2 Ein- und Ausschalten des gesamten Systems

C.1.2.1 Gesamtes System einschalten

Hinweis: Die im Folgenden beschriebenen Prozeduren zeigen Beispiel-Bildschirme von Fenstern, wie sie bei der PRIMEQUEST 580A/540A*/580/540/480/440 erscheinen.

Vorgehensweise

1 Schalten Sie das MMB und die Peripheriegeräte ein.

2 Melden Sie sich beim MMB Web-UI an.
Das Fenster des MMB Web-UI wird angezeigt.

3 Wählen Sie [System] → [System Power Control] aus dem Menü des MMB.
Das Fenster [System Power Control] wird angezeigt.

*: wird von Fujitsu Technology Solutions nicht unterstützt

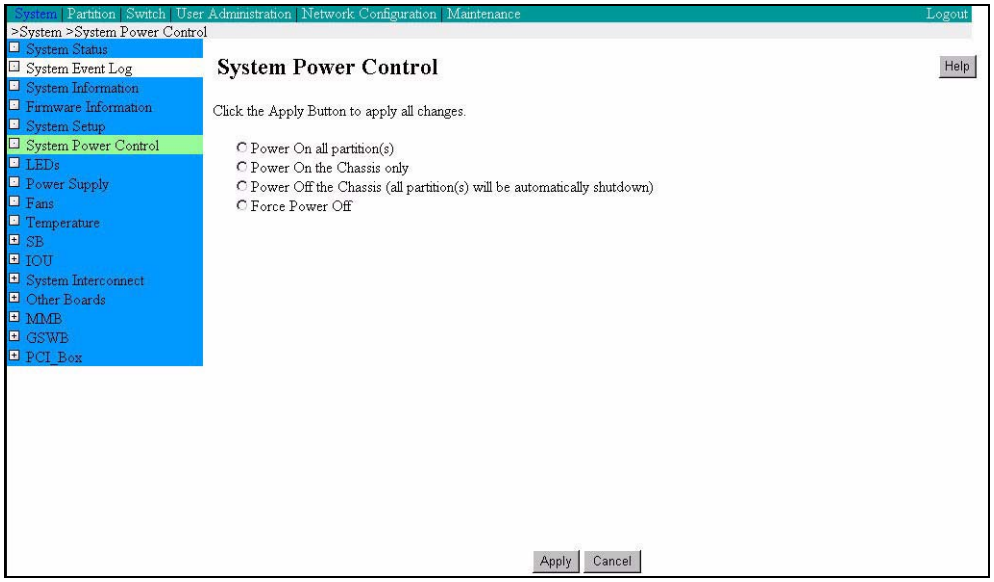


Abbildung C.5 Das Fenster [System Power Control]

4 Aktivieren Sie das Optionsfeld [Power On all partition(s)] oder [Power On the Chassis only] (nur bei PRIMEQUEST 580A/540A*/580/540/480/440), und klicken Sie dann auf [Apply].
Das System wird eingeschaltet.

Anm.: Wenn [Power On all partition(s)] ausgewählt wird, während nur der Schrank eingeschaltet ist, wird die Stromversorgung zu sämtlichen Partitionen eingeschaltet.
Wenn [Power On the Chassis only] gewählt wird, wird die Stromversorgung zu den Komponenten außer dem Systemboard (SB) und der IO Unit eingeschaltet (inkl. dem GSWB).

*: wird von Fujitsu Technology Solutions nicht unterstützt

Erläuterung des Fensters [System Power Control]

Tabelle C.1 Ein- und Ausgabe von Daten im Fenster [System Power Control]

Position	Beschreibung
Power On all partition(s)	Jede Partition wird eingeschaltet. Wenn diese Option ausgewählt wird, während nur der Schrank eingeschaltet ist, werden die Partitionen alle eingeschaltet.
Power On the Chassis only (PRIMEQUEST 580A/ 540A*/580/540/480/440 only)	Alle Komponenten mit Ausnahme des Systemboards und der IO Units werden eingeschaltet. Diese Operation schließt auch das GSWB ein.
Power Off the Chassis (all partition(s) will be automatically shutdown).	Alle Partitionen und Schränke werden ausgeschaltet. Die Option bleibt ohne Wirkung, wenn Sie sie bei ausgeschaltetem System wählen.
Force Power Off	Die Partitionen werden ausgeschaltet, ohne sie zuvor herunterzufahren.

*: wird von Fujitsu Technology Solutions nicht unterstützt

C.1.2.2 Gesamtes System ausschalten

⚠ ACHTUNG

Datenverlust

Stellen Sie vor dem Ausschalten sicher, dass folgende Maßnahmen ergriffen wurden, um einen Datenverlust zu vermeiden:

- Alle Anwendungen wurden geschlossen.
- Alle Benutzer sind abgemeldet.

Hinweis: Eine Partition, auf der Windows installiert ist, wird möglicherweise nicht heruntergefahren werden, wenn die Shutdown-Funktion aus dem MMB Web-UI heraus ausgeführt wird. Benutzen Sie die Shutdown-Funktion von Windows, um die Partition auszuschalten. Näheres über die Shutdown-Funktion von Windows finden Sie im *PRIMEQUEST 500/400 Series Reference Manual: GUI/Commands* (U41633-J-Z816-x-76/C122-E003EN).

Hinweis: Die im Folgenden beschriebenen Prozeduren zeigen Beispiel-Bildschirme von Fenstern, wie sie bei der PRIMEQUEST 580A/540A*/580/540/480/440 erscheinen.

Vorgehensweise

1 Melden Sie sich bei dem MMB Web-UI an.
Das Fenster des MMB Web-UI wird angezeigt.

2 Wählen Sie [System] → [System Power Control] aus dem MMB-Menü.
Das Fenster [System Power Control] wird angezeigt.

*: wird von Fujitsu Technology Solutions nicht unterstützt

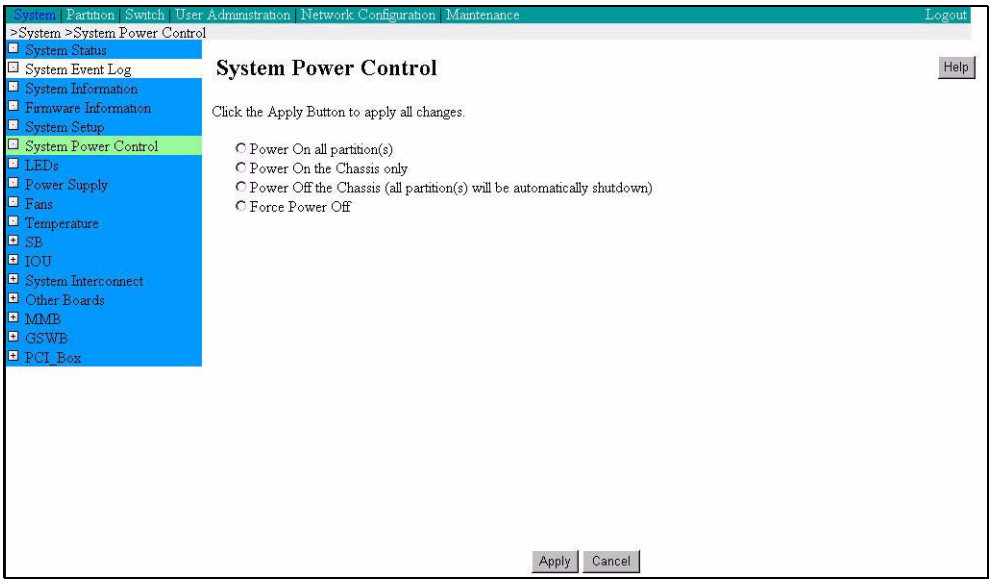


Abbildung C.6 Das Fenster [System Power Control]

3 Wählen Sie [Power Off the Chassis (all partition(s) will be automatically shutdown)] oder [Force Power Off], und klicken Sie auf [Apply], um Ihre Wahl zu bestätigen.

Das System wird ausgeschaltet.

Anm.: Wenn Sie [Force Power Off] wählen, wird das System ausgeschaltet, ohne dass zuvor eventuell in den Partitionen laufende Betriebssysteme heruntergefahren werden.

C.2 Schränke und Partitionen ein- und ausschalten

Dieser Abschnitt beschreibt das Ein- und Ausschalten für das gesamte PRIMEQUEST System und für die Partitionen.

Hinweis: Eine Partition, auf der Windows installiert ist, wird möglicherweise nicht heruntergefahren werden, wenn die Shutdown-Funktion aus dem MMB Web-UI heraus ausgeführt wird. Benutzen Sie die Shutdown-Funktion von Windows, um die Partition auszuschalten. Näheres über die Shutdown-Funktion von Windows finden Sie im *PRIMEQUEST 500/400 Series Reference Manual: Basic Operation/GUI/Commands: GUI/Commands* (U41633-J-Z816-x-76/C122-E003EN).

Hinweis: Die im Folgenden beschriebenen Prozeduren zeigen Beispiel-Bildschirme von Fenstern, wie sie bei der PRIMEQUEST 580A/540A*/580/540/480/440 erscheinen.

Vorgehensweise

1 Wählen Sie [System] → [System Power Control] aus dem MMB-Menü.
Das Fenster [System Power Control] wird angezeigt.

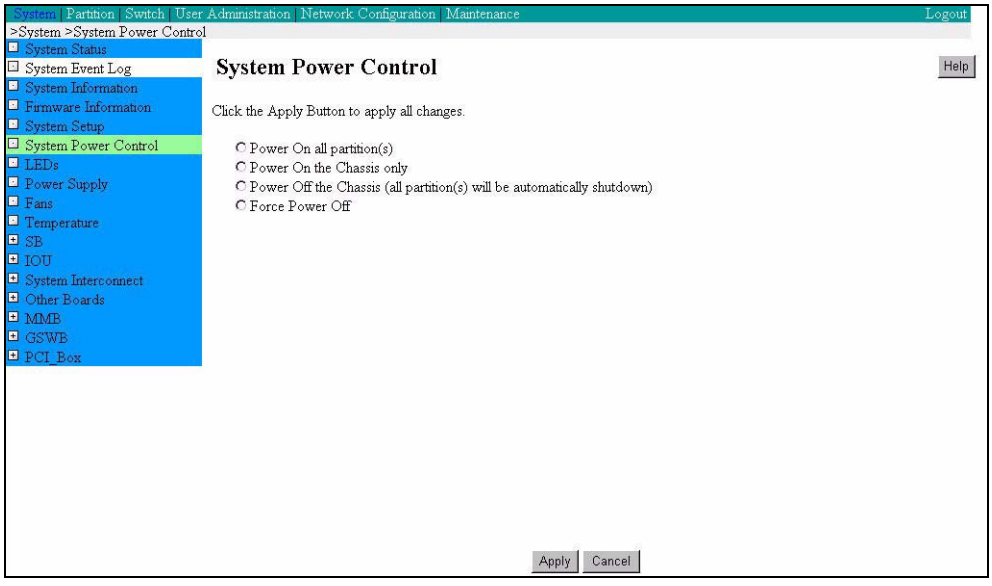


Abbildung C.7 Das Fenster [System Power Control]

2 Wählen Sie eine Option aus und klicken Sie auf [Apply].

*: wird von Fujitsu Technology Solutions nicht unterstützt

3 Wenn Sie [Power Off the Chassis (all partition(s) will be automatically shut-down)] oder [Force Power Off] wählen, erscheint ein Bestätigungsfenster. Klicken Sie hier auf [OK], um den Prozess zu starten oder auf [Cancel], um zum Hauptfenster zurückzukehren, ohne den Prozess zu starten.

Erläuterung des Fensters [System Power Control]

Tabelle C.2 Ein- und Ausgabe von Daten im Fenster [System Power Control]

Position	Beschreibung
Power On all partition(s)	Alle Partitionen werden eingeschaltet. Wenn diese Option ausgewählt wird, während nur der Schrank eingeschaltet ist, werden die Partitionen alle eingeschaltet.
Power On the Chassis only (nur bei PRIMEQUEST 580A/540A*/580/540/480/440)	Alle Komponenten mit Ausnahme des Systemboards und der IO Units werden eingeschaltet. Diese Operation schließt auch das GSWB ein.
Power Off the Chassis (all partition(s) will be automatically shut down.)	Alle Partitionen und der Schrank werden ausgeschaltet.
Force Power Off	Das System wird ausgeschaltet, ohne die Partitionen zuvor herunterzufahren.

*: wird von Fujitsu Technology Solutions nicht unterstützt

C.3 Partitionen ein- und ausschalten

Dieser Abschnitt beschreibt die folgenden Ein- und Ausschaltverfahren für die Partitionen:

- Partition einschalten (→ C.3.1)
- Partition ausschalten (→ C.3.2)

Für diese Operation sind Systemverwalterrechte erforderlich.

C.3.1 Partition einschalten

In diesem Abschnitt wird das Einschalten einer Partition beschrieben.

Vorgehensweise

1 Melden Sie sich beim MMB Web-UI.
Das Fenster MMB Web-UI wird angezeigt.

2 Wählen Sie [Partition] → [Power Control] aus dem MMB-Menü.
Das Fenster [Power Control] wird angezeigt. Hier werden nur die Partitionen angezeigt, die hochgefahren werden können.

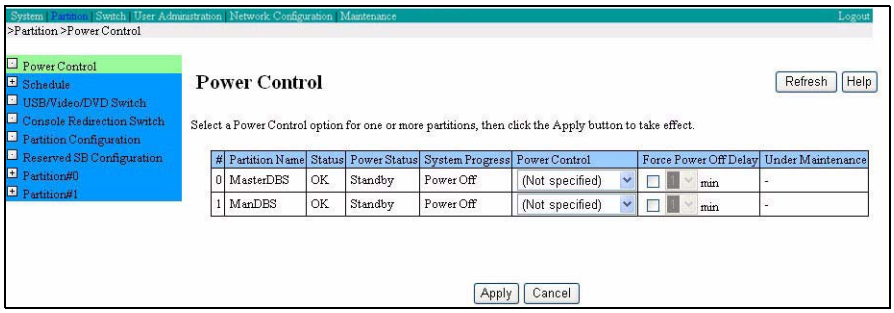

System | Partition | Switch | User Administration | Network Configuration | Maintenance
Logout
>Partition >Power Control
Power Control
Schedule
USB/Video/DVD Switch
Console Redirection Switch
Partition Configuration
Reserved SB Configuration
Partition#0
Partition#1
Power Control
Refresh
Help
Select a Power Control option for one or more partitions, then click the Apply button to take effect.
| Partition Name | Status | Power Status | System Progress | Power Control | Force Power Off Delay | Under Maintenance
0 | MasterDBS | OK | Standby | Power Off | (Not specified) | min | -
1 | ManDBS | OK | Standby | Power Off | (Not specified) | min | -
Apply
Cancel

Abbildung C.8 Das Fenster [Power Control]

Die Spalte „#“ enthält die Partitionsnummer.
Näheres über das Fenster [Power Control] finden Sie in Teil III, „MMB“ des *PRIMEQUEST 500/400 Series Reference Manual: Basic Operation/GUI/Commands* (U41633-J-Z816-x-76/C122-E003EN).

3 Um eine Partition einzuschalten, wählen Sie in der Spalten [Power Control] die Option [Power On] und klicken Sie dann auf [Apply].
Ein Bestätigungsfenster wird angezeigt. Klicken Sie auf [OK], um fortzufahren oder auf [Cancel], um abzubrechen.
Hinweis: Wenn der Vorgang nicht durchgeführt werden kann, weil die betreffende Partition bereits eingeschaltet ist oder weil sie gerade abgeschaltet wird, erscheint ein entsprechender Warnhinweis.

Erläuterung des Fensters

Tabelle C.3 Ein- und Ausgabe von Daten im Fenster [Power Control]

Feld	Beschreibung
#	Die Nummer der jeweiligen Partition wird angezeigt. Es werden nur Partitionen angezeigt, denen ein Systemboard bzw. eine IO Unit zugewiesen ist.
Partition Name	Der Name der jeweiligen Partition wird angezeigt.
Status	Status der jeweiligen Partition wird angezeigt: • [OK]: Die Partition funktioniert ordnungsgemäß. • [Degraded]: Eine Komponente ist fehlerhaft (die Partition kann eine fehlerhafte Komponente isolieren und weiterarbeiten). • [Warning]: Die Partition gibt eine Warnung aus (ein Ausfall ist zu erwarten). • [Failed]: Die Partition ist ausgefallen.
Power Status	Der Einschaltstatus der Partition wird angezeigt: • [On]: Die Partition ist eingeschaltet. • [Standby]: Die Partition befindet sich im Standby-Modus.

Tabelle C.3 Ein- und Ausgabe von Daten im Fenster [Power Control]

Feld	Beschreibung
System Progress	Der Fortschritt der Partition wird angezeigt: • [Power Off]: Die Partition ist ausgeschaltet. • [Power On In Progress]: Die Partition wird gerade eingeschaltet. • [Reset]: Die Partition wird neu gestartet. • POST XXXXh: zeigt an, dass POST Code = XXXXh gerade verarbeitet wird. • [Boot]: Status der Partition: - Bootvorgang ist gestartet - PSA ist noch nicht installiert - Installation ist gestartet - Sicherung oder Wiederherstellung durch SystemcastWizard ist gestartet • [OS Running]: Das Betriebssystem ist aktiv. • [OS Shutdown]: Das Betriebssystem ist heruntergefahren. • [Panic]: Das System befindet sich im Panic-Modus. • [Power Off In Progress]: Die Partition wird ausgeschaltet. • [Check Stop]: Die Partition ist ausgeschaltet. • [Initiate soft-shutdown]: Der Countdown zu einem erzwungenen Ausschalten beginnt.

Tabelle C.3 Ein- und Ausgabe von Daten im Fenster [Power Control]

Feld	Beschreibung
Power Control	Der Benutzer kann ein Ein-/Ausschaltverfahren wählen. Bei einer eingeschalteten Partition wird die Option [Power On] nicht angeboten. Bei einer ausgeschalteten Partition werden die Optionen [Power Off], [Reset], [INIT], [Power Cycle] und [Force Power Off] nicht angeboten. • [Power On]: Schaltet die Partition ein. • [Power Off]: Schaltet die Partition aus. Diese Option bewirkt dasselbe wie die Betätigung des Ein-/Ausschalters der Einheit. Wenn das Betriebssystem ACPI (Advanced Configuration and Power Interface) unterstützt, wird es bei [Power Off] heruntergefahren bevor die Partition ausgeschaltet wird. Näheres finden Sie in der Beschreibung von ACPI. Wenn das Betriebssystem ACPI nicht unterstützt, schaltet diese Option die Partition aus, ohne das Betriebssystem vorher herunterzufahren. • [Power Cycle]: Erzwingt das Aus- und Wiedereinschalten der Partition. • [Reset]: Führt einen Neustart der Partition durch. • [INIT]: Setzt einen INIT Interrupt an die Partition ab. • [Force Power Off]: Erzwingt ein Ausschalten der Partition. • [Not specify]: Keine Aktion für die Partition festgelegt. Hinweise: • Mit INIT wird das Beenden aller auf der Partition laufenden Anwendungen erzwungen. Schließen Sie wichtige Anwendungen, bevor Sie ein INIT ausführen. Hängen Sie ferner alle nicht benötigten Dateisysteme aus.
Force Power Off Delay	Bei Wahl der Option [Power Off] kann das Ausschalten der Partition fehlschlagen, wenn das Betriebssystems der relevanten Partiton nicht ordnungsgemäß herunter-gefahren wird. Es kann eine Verzögerung von 1 bis 9 Minuten festgelegt werden. Nach Ablauf dieses Zeitraums wird das Ausschalten der Partition erzwungen. Voreinstellung: nicht aktiviert

Tabelle C.3 Ein- und Ausgabe von Daten im Fenster [Power Control]

Feld	Beschreibung
Under Maintenance	Zeigt an, ob die Partition aktuell gewartet wird: [Maintenance]: Die Partition wird aktuell gewartet. [- (Bindestrich)]: Die Partition wird nicht gewartet. Für Partitionen, die gewartet werden, können keine Einstellungen vorgenommen werden. Hinweis: Abhängig von der MMB-Firmware-Version wird bei der Serie PRIMEQUEST 500A/500 das Feld „Under Maintenance“ im Fenster [Power Control] eventuell nicht ausgegeben. In diesem Fall wird die Nummer der gewarteten Partition unter „Under Maintenance“ im Informationsbereich ausgegeben.

Hinweis: Wenn das Betriebssystem ACPI (Advanced Configuration and Power Interface) unterstützt, wird es heruntergefahren, bevor die Partition ausgeschaltet wird. Wenn es ACPI aber nicht unterstützt, wird die Partition ausgeschaltet, ohne dass zuvor das Betriebssystem heruntergefahren wird. Auch wenn das Betriebssystem ACPI unterstützt, kann das Ausschalten der Partition fehlschlagen, wenn eine auf dem Betriebssystem laufende Anwendung ACPI ihrerseits nicht unterstützt. Näheres finden Sie im Handbuch des Betriebssystems oder der jeweiligen Anwendungen.

Anm.: Nachdem ein Schrank ausgeschaltet wurde, kann er einige Zeit nicht wieder eingeschaltet werden. Während dieser Zeit ist [Power Control] ausgegraut, also nicht verfügbar.

C.3.2 Partition ausschalten

Dieser Abschnitt beschreibt, wie eine Partition ausgeschaltet wird.

- Eine Partition, auf der Windows installiert ist, wird möglicherweise nicht heruntergefahren werden, wenn die Shutdown-Funktion aus dem MMB Web-UI heraus ausgeführt wird. Benutzen Sie die Shutdown-Funktion von Windows, um die Partition auszuschalten. Näheres über die Shutdown-Funktion von Windows finden Sie im *PRIMEQUEST 500/400 Series Reference Manual: Basic Operation/GUI/Commands*(U41633-J-Z816-x-76/C122-E003EN).
- Unter folgenden Umständen ziehen Sie bitte einen Kundendienst-Techniker hinzu. Führen Sie auch keinen [Reset] oder [Force Power Off] für eine Partition aus, bevor das Problem gelöst ist:
  [Power off], [Reset], oder [Force Power Off] wird für eine Partition ausgeführt oder ein shutdown-Kommando wird ausgeführt, und anschließend wird als [Status] im Info-Bereich des MMB-Web-UI „Error“ angezeigt. Beim Versuch, den Status jeder Komponente im MMB-Web-UI anzeigen zu lassen, wir bei [Part Number] oder [Serial Number] „Read Error“ angezeigt.

Vorgehensweise

1 Melden Sie sich beim MMB Web-UI an.
Das Fenster des MMB Web-UI wird angezeigt.

2 Wählen Sie [Partition] → [Power Control] aus dem MMB-Menü.
Das Fenster [Power Control] wird angezeigt.

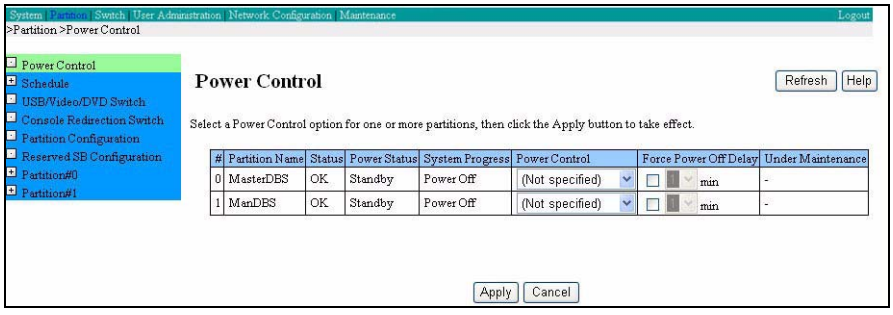


Abbildung C.9 Das Fenster [Power Control]

Die Spalte „#“ enthält die Nummer der Partition.

3 Um eine Partition auszuschalten, wählen Sie in der Spalte [Power Control] die Option [Power Off] und klicken Sie auf [Apply].
Die Partition wird ausgeschaltet.

Hinweis:Aus den unten beschriebenen Gründen muss das Herunterfahren einer Partition vom Betriebssystem aus durchgeführt werden.
Wird die Operation [Power Off] ausgewählt und das Betriebssystem unterstützt ACPI, kann das Betriebssystem heruntergefahren und eine Partition durch die Operation power-off wie oben beschrieben, abgeschaltet werden. Wenn jedoch das Betriebssystem ACPI nicht unterstützt, wird die Partition ausgeschaltet, ohne dass zuvor das Betriebssystem heruntergefahren wird.
Auch wenn das Betriebssystem ACPI unterstützt, kann das Ausschalten der Partition fehlschlagen, wenn eine auf dem Betriebssystem laufende Anwendung ACPI ihrerseits nicht unterstützt. Näheres finden Sie im Handbuch des Betriebssystems oder der jeweiligen Anwendungen.

Anhang D SAN Boot Environment

In diesem Anhang wird beschrieben, wie ein SAN Boot Environment bei Windows eingerichtet wird.

D.1 Voraussetzungen

Für die Einrichtung einer SAN Boot Environment müssen die unten aufgeführten Hardware- und Softwarevoraussetzungen erfüllt sein.

In dem hier verwendeten Beispiel wird das Fujitsu Speicherprodukt ETERNUS* verwendet. Die grundlegenden Einstellungen treffen jedoch auch für die SAN-Speichereinheiten anderer Anbieter zu.

- PRIMEQUEST
- Fibre Channel-Karte (FC-Karte)
- SAN-Speichereinheit (ETERNUS*)
- FC-Switch (gemäß der geplanten Konfiguration)
- PC, um die Konfiguration der SAN-Speichereinheit (ETERNUS*) und des FC-Switches durchzuführen (kann auch als MMB-Konsole oder sonstige Konsole dienen)
- Windows Server 2003, Enterprise Edition für Itanium-basierte Systeme oder Windows Server 2003, Datacenter Edition für Itanium-basierte Systeme
- USB-Diskettenlaufwerk
  (Installation über KVM-Einheit)

*: Angebot und Support in EMEA nur für die globalen Kunden von Fujitsu

D.2 SAN Boot Environment einrichten

Gehen Sie wie folgt vor, um eine SAN Boot Environment einzurichten:

- SAN Boot Environment konzipieren
  Planen Sie die Boot-Umgebung einschließlich der Standorte für die PRIMEQUEST und die SAN-Speicher, der Verbindungen und der IP-Adressen. Der erreichbare Grad an Zuverlässigkeit hängt in einem hohen Maße von der Topologie der PRIMEQUEST, der SAN-Speicher und der FC-Switches ab. Planen Sie die Umgebung gemäß Ihren Anforderungen.
- SAN-Einstellungen für die PRIMEQUEST festlegen.
  Richten Sie die SAN-Speichereinheiten und die PRIMEQUEST gemäß der geplanten Konfiguration ein. Der Fibre Channel EFI-Treiber muss ebenfalls konfiguriert werden.
- SAN-Speicher und FC-Switches einrichten
  Nun müssen die SAN-Speichereinheiten und FC-Switches gemäß dem Anschlussplan eingerichtet, verbunden, konfiguriert und abgestimmt werden.

D.3 Planung

Die Topologie der SAN Boot Environment ist von der Größe des Unternehmens abhängig.

In diesem Abschnitt werden zwei empfohlene Konfiguration einer SAN Boot Environment für Windows-Systeme beschrieben: 2-Wege- und 4-Wege-Konfiguration.

Hinweise:

- Wegen ihrer hohen Zuverlässigkeit wird eine 4-Wege-Konfiguration empfohlen. Die Konfiguration in unserem Beispiel muss an die Größe Ihres Unternehmens angepasst werden.
- Die in diesem Abschnitt beschriebene Beispielkonfiguration verwendet FC-Karten. Sie muss gegebenenfalls geändert werden, um zusätzliche Karten zu berücksichtigen.

(1) Empfohlene 2-Wege-Konfiguration

Abbildung D.10 stellt die SAN Boot Environment in einer 2-Wege-Konfiguration dar.

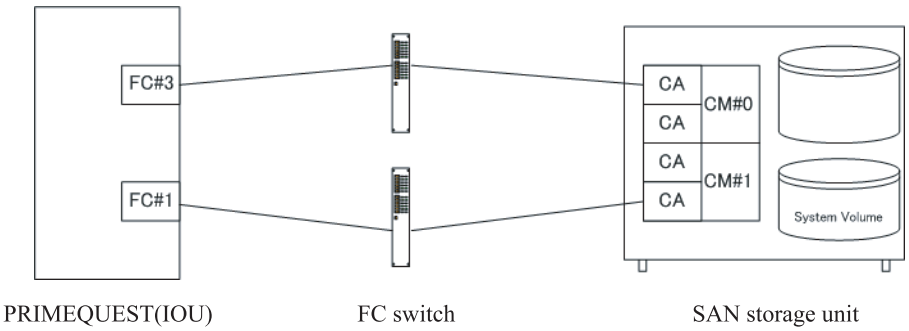


Abbildung D.10 Beispiel für eine SAN 2-Wege-Konfiguration

(2) Empfohlene 4-Wege-Konfiguration

Abbildung D.11 stellt die SAN Boot Environment in einer 4-Wege-Konfiguration dar.

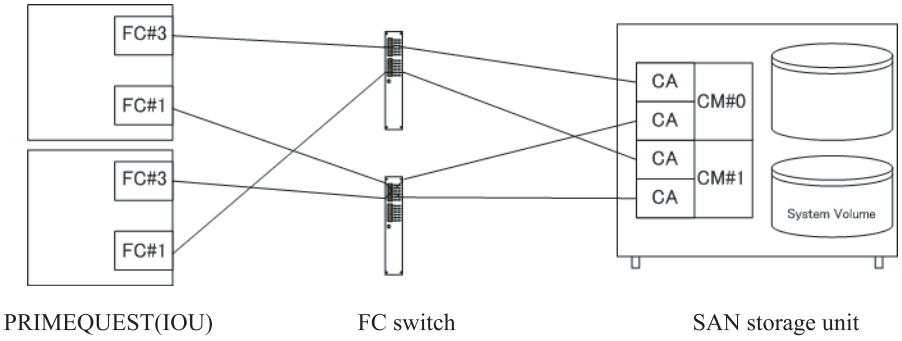


Abbildung D.11 Beispiel für eine SAN 4-Wege-Konfiguration

D.3.1 Planungshinweise

Bei der Planung der SAN-Umgebung sollten folgende Punkte beachtet werden:

- Einschränkungen bei den Steckplätzen für FC-Karten
  PRIMEQUEST 580A/540A/580/540
  - In einer SAN Boot-Konfiguration kann das Betriebssystem über jeden beliebigen Slot eines Ein-/Ausgabegeräts installiert werden. Wenn nach der Installation des Betriebssystems Multipath-Einstellungen auch für den Slot dieser Installation gemacht werden, ist SAN Boot jedoch für alle Slots der Ein-/Ausgabegeräte verfügbar.
  - In einer SAN Boot-Konfiguration können das Betriebssystem von einer PCI-Box nicht installiert und SAN-Boot nicht ausgeführt werden.

  PRIMEQUEST 480/440
  - Verbinden Sie die FC-Karte (HBA) für das SAN Boot in der PRIMEQUEST 480/440 mit dem PCI-Slot 1 oder 3.
  - In einer SAN Boot-Konfiguration können das Betriebssystem von einer PCI-Box nicht installiert und SAN-Boot nicht ausgeführt werden.

  PRIMEQUEST 520A/520/420
  In einer SAN Boot-Konfiguration können Betriebssysteminstallation und SAN-Boot von jedem PCI-Steckplatz ausgeführt werden, in dem ein FC-Controller eingebaut ist.
- Wählen Sie 1-zu-1 WWPN für das Zoning.
  Bei Verwendung von FC-Switches muss das Zoning gemäß der Systemkonfiguration eingerichtet werden. Bei manuellem Zoning kann entweder ein spezifischer Port oder WWPN eingesetzt werden. Der Einfachheit halber sollte jedoch 1-zu-1 WWPN gewählt werden. Wenn ein spezifischer Port benutzt wird und ein CA (Host/FC-Switch-Port einer ETERNUS*-Einheit) ausfällt, muss das Zoning neu eingerichtet werden.
- Kein Sharing der Systemplatte.
  Die Systemplatte darf nicht von mehreren Servern gemeinsam genutzt werden. Nutzen Sie die Host-Affinity-Funktion, um eine exklusive Steuerung der Systemplatte zu gewährleisten. Wenn Sie SAN-Speichereinheiten eines anderen Anbieters verwenden wollen, stellen Sie sicher, dass diese eine vergleichbare Funktion anbieten.
- Einschränkungen bei der Nutzung des ETERNUS* Multipath-Treibers
  1 Wenn der ETERNUS* Multipath-Treiber benutzt wird, müssen die einzelnen logischen Einheiten (LUNs) in der ETERNUS*-Einheit allen HBAs eines Servers gleichermaßen zugewiesen werden.

*: Angebot und Support in EMEA nur für die globalen Kunden von Fujitsu

2 Wenn 1-zu-1 WWPN nicht verwendet wird, können mögliche Konfigurationen nicht über einen FC-Switch von einem HBA aus auf mehrere CAs innerhalb desselben Schranks zugreifen.

3 Die Anzahl Pfade ist begrenzt.
Unter Windows sind maximal 8 Pfade konfigurierbar.

Näheres finden Sie im Handbuch zum ETERNUS* Multipath-Treiber.

*: Angebot und Support in EMEA nur für die globalen Kunden von Fujitsu

D.4 Einstellungen

Dieser Abschnitt umreißt die Einstellungen für die ETERNUS* Systemeinheit. Näheres finden Sie in den zum Lieferumfang der ETERNUS gehörenden Handbüchern.

D.4.1 Bereiche reservieren (RAID-Gruppen, logische Einheiten)

Reservieren Sie die Bereiche, die auf der ETERNUS* für die Einrichtung der SAN Boot Environment erforderlich sind. Diese Bereiche unterliegen keinen spezifischen Einschränkungen. Näheres über das Reservieren der erforderlichen Bereiche ist in den Handbüchern der ETERNUS* beschrieben.

D.4.2 Einstellungen für logische Einheiten vornehmen

Weisen Sie den reservierten Bereich einer logischen Einheit einer CA zu.

Verwenden Sie dazu die entsprechende ETERNUS* Installationssoftware. Näheres ist in den Handbüchern der ETERNUS* beschrieben.

Es stehen zwei Muster für die Zuweisung zur Verfügung:

- Wenn der Zugang zu einem Host Bus Adapter (HBA) bereits verfügbar ist (etwa wenn die ETERNUS* direkt an den HBA angeschlossen ist), kann der für die Einstellung erforderliche WWPN des HBAs aus der Liste entnommen werden, die von der Installationssoftware der ETERNUS* angeboten wird.

  Hinweis: Die E-/A-Verarbeitung über die ETERNUS*-Einheit muss mindestens ein Mal über den HBA durchgeführt werden.

- Wenn der Zugang zu einem HBA nicht bereits verfügbar ist, müssen die benötigten Angaben über die EFI-Konsole des Servers ermittelt werden, in dem der HBA installiert ist. Näheres finden Sie im Abschnitt „EFI-Treiber konfigurieren“.

*: Angebot und Support in EMEA nur für die globalen Kunden von Fujitsu

Beachten Sie bezüglich der Einstellungen für logische Einheiten folgendes:

- Verwenden Sie die Sicherheitsfunktion.
  Verwenden Sie die Host Affinity-Funktion, um die Anzahl der Server einzugrenzen, die auf die einzelnen Laufwerke zugreifen können. Wenn beispielsweise eine ETERNUS*-Einheit von zwei Partitionen gemeinsam genutzt wird und wenn jede Partition eine eingene Systemplatte und eine gemeinsam genutzte Platte besitzt, sollten nur bestimmte Server (HBAs) auf die Platte zugreifen können, damit die Systemplatte geschützt ist.

D.4.3 FC-Switch einrichten

Dei FC-Switches für die ETERNUS* SN200 Serie werden in der Regel von einem Telnet-Terminal aus über eine Verbindung zum Betriebssystem der ETERNUS* SN200 eingerichtet (gewöhnlicher PC genügt).

Im Folgenden ist mit Switch ein FC-Switch gemeint.

1 Vorbereitungen
  Ermitteln Sie die WWPNs der ETERNUS* und des HBAs.
  Benutzen Sie dazu ETERNUS* mgr und wählen Sie aus dem Status-Menü die WWPN-Listfunktion, die die den CAs zugewiesenen WWPNs aufführt. Näheres finden Sie in den Handbüchern der ETERNUS*.
  Eine genaue Beschreibung, wie Sie die WWPN des HBAs ermitteln können, finden Sie im Abschnitt D.4.4, „EFI-Treiber konfigurieren“.

2 Grundlegende Einstellungen des Switchs
  Es müssen die IP-Adresse des LAN, die Teilnetzmasken und Gateway-Adressen des Switchs und des PCs eingestellt werden. Diese Einstellungen können über das Bedienfeld oder über den seriellen Port vorgenommen werden. Näheres finden Sie in den Referenzhandbüchern der ETERNUS* SN200 Serie.
  Ferner muss die SNMP-Funktion für den Switch durch die erforderliche Einstellung aktiviert werden. Wenn für den Switch das Zoning bereits eingerichtet wurde, ist dies jedoch nicht mehr erforderlich.

3 Einrichten der Zonen und der Konfiguration sowie Überprüfung der Konfiguration
  Legen Sie die Zonen mit ihren entsprechenden Konfigurationen an und überprüfen Sie diese. Näheres über diese Maßnahmen finden Sie im Benutzerhandbuch der ETERNUS*.

*: Angebot und Support in EMEA nur für die globalen Kunden von Fujitsu

D.4.4 EFI-Treiber konfigurieren

Um das System von einer SAN-Speichereinheit aus starten zu können, führen Sie für jeden HBA die im Folgenden beschriebenen Schritte durch.

Der EFI-Treiber, der verwendet werden muss, hängt von der installierten FC-Karte ab. Die Bildschirmanzeigen für die verschiedenen Treiberversionen sind unterschiedlich. Dieser Abschnitt beschreibt das Vorgehen für jede Version.

- EFI-Treiber (Version 3.10a6) konfigurieren (→D.4.4.1)
- EFI-Treiber (Version 3.11a4/ Version 3.11x1 konfigurieren) (→D.4.4.2)

D.4.4.1 EFI-Treiber (Version 3.10a6) konfigurieren

1 Schalten Sie die Partition ein.
Auf der Konsole wird der [EFI Boot Manager] angezeigt.

```
EFI Boot Manager ver x.xx [x.xx]

Please select a boot option

    EFI Shell [Built-in]
    DVD/Acpi(PNP0A03, 0)/Pci(1D|1)/Usb(0, 0)/Usb(1, 0)
    Network/Acpi(PNP0A03,0)/Pci(1E|0)/Pci(8|0)/Mac(000B5D6F80A9)
    Boot Option Maintenance Menu
    Setup Menu
```

2 Starten Sie die EFI-Shell.
Wählen Sie die Option [EFI Shell (Built-in)] und drücken Sie die [Enter]-Taste.
Die EFI-Shell wird gestartet.

3 Rufen Sie eine Liste der Treiber auf.
Geben Sie in der EFI-Shell folgendes Kommando ein und drücken Sie die [Enter]-Taste:

```
Shell> drivers -b
```

Eine Liste der Treiber ähnlich der nachfolgend dargestellten wird angezeigt. Suchen Sie nach dem Eintrag mit dem Text „Emulex SCSI Pass Thru Driver“ in der Spalte DRIVER NAME und notieren Sie den Wert, der in der Spalte DRV angezeigt wird. Im folgenden Beispiel ist die ID-Nummer des Treibers 22.

Überprüfen Sie die VERSION-Information in der folgenden Liste:

```
Shell> drivers -b
             T   D
D            Y C I
R            P F A
V   VERSION  E G G #D #C  DRIVER NAME                          IMAGE NAME
=== ======== = = = == === ============================== ================
00D 00000010 B - -  2  43 PCI Bus Driver                       PciBus

020 00000010 B - -  3   3 USB Bus Driver                       UsbBus
021 00000010 D - -  1   - Usb Keyboard Driver                 UsbKeyboard
022 00031114 B X X  2   7 Emulex SCSI Pass Thru Driver        Elxcli311a4
Press ENTER to continue, 'q' to exit: q

Shell>
```

Hinweis: Die oben wiedergegebenen Informationen, einschließlich der ID-Nummern, variieren je nach der jeweiligen Umgebung.

4 Liste der HBAs anzeigen.

Geben Sie „drvcfg -s X“ ein, wobei X die im vorherigen Schritt 3 ermittelte ID-Nummer des Treibers ist und drücken Sie die [Enter]-Taste. Eine Liste der installierten FC-Karten ähnlich der folgenden wird angezeigt.

```
          Emulex FC EFI-Bios Utility, Ver: 3.10a6
-------------------------------------------------------------
      Emulex Adapters in this System: 001 thru 002

 001: LP10k     PCI-X  133MHz Bus#: 49 Dev#: 01 Func#: 00
 002: LP10k     PCI-X  100MHz Bus#: 4B Dev#: 02 Func#: 00
```

Hinweis: Die Positionen der physikalischen Slots können entsprechend den im Fenster angezeigten Bus-Nummern und der Tabelle von PRIMEQUEST zu physikalischer Position - Bus-Nummer ermittelt werden. Stellen Sie sicher, dass sie übereinstimmen.
Die Tabelle von PRIMEQUEST zu physikalischer Position - Bus-Nummer finden Sie in Kapitel 4, „Physical Positions and Bus Numbers“, im Handbuch *Reference Manual: Tool/Operation Information* (C122-E074EN/ U41757-J-Z816-x-76).
PRIMEQUEST 580A/540A/580/540/480/440
→ „PRIMEQUEST 580A/540A/580/540/480/440 PCI Slot Physical Positions and Bus Numbers“
PRIMEQUEST 520A/520/420
→ „PRIMEQUEST 520A/520/420 PCI Slot Physical Positions and Bus Numbers“

5 Wählen Sie den HBA aus.

Setzen Sie den Cursor mit den Cursor-Tasten in der Liste der HBAs auf den Eintrag, der für die SAN Boot Environment benutzt werden soll, und drücken Sie die [Enter]-Taste. Es wird das Setup Utility-Menü angezeigt.

```
         Emulex FC EFI-Bios Utility, Ver: 3.10a6
-------------------------------------------------------------
 001: LP10k     PCI-X  133MHz Bus#: 49 Dev#: 01 Func#: 00
    HBA Status: Ready              Boot Bios : Disabled
    EFI  Boot : TE3.10A6           Firmware  : TS1.91A1
-------------------------------------------------------------
                     1. Setup Utility
                     2. Firmware Update
```

6 Anzeige des Menüs des HBA Setup Utilitys

Wählen Sie [1. Setup Utility] und drücken Sie [Enter]. Es wird das folgende Menü angezeigt.

```
        Emulex FC EFI-Bios Setup Utility, Ver: 3.10a6
-----------------------------------------------------------------
   001: LP10k     PCI-X  133MHz Bus#: 49 Dev#: 01 Func#: 00
 Boot Bios : Disabled  Firmware  : TS1.91A1  I/O Base  : 8300
 Port Name : 10000000C942E2D6  Node Name : 20000000C942E2D6
 S_ID      : 000000    Link Speed: NA        Topology  : Invalid
-----------------------------------------------------------------
                1. Enable or Disable BIOS
                2. Configure HBA Parameters
                3. Configure Boot Parameters
                4. Reset to Default Values
```

7 Ermitteln der WWPN des HBAs

Die WWPN des HBAs wird im menü (Schritt 6) als „Port Name“ angezeigt.

8 Aktivieren Sie die Einstellungen für den HBA.

Wählen Sie im Menü (Schritt 6) [4. Reset to Default Values].

Geben Sie in der erscheinenden Dialogbox „y“ ein.

```
Do you want to Force defaults (y/n) :
```

Hinweis: Unmittelbar nach Auslieferung des Systems ist dieser Schritt nicht erforderlich, da die Einstellung bereits erfolgt ist.

9 Aktivieren Sie die BIOS Boot Option.

Wählen Sie im Menü (Schritt 6) [1. Enable or Disable BIOS].

Es wird das folgende Menü angezeigt:

```
 EFI-Bios Boot Option is Currently DISABLED.
             Disabled - default
             Enabled
```

Wählen Sie [Enabled].

10 Drücken Sie einmal die [Esc]-Taste um zum Bildschirm von Schritt 6 zurückzukehren.

11 Geben Sie das Boot-Gerät an.
Wählen Sie im Menü (Schritt 6) [3. Configure Boot Parameters].
Es wird das folgende Menü angezeigt:

```
1. Device Path Selection
2. Maximum Luns/Target
3. Boot Target Scan
4. Configure Boot Devices
5. Delay Device Dicovery
```

12 Wählen Sie [4. Configure Boot Devices]. Es wir eine Datenliste wie im folgenden gezeigt ausgegeben. Wählen Sie einen leeren Eintrag. Bei Auslieferung des Sytems sind alle Einträge leer.

```
01: DID:000000 WWN:00000000 00000000
02: DID:000000 WWN:00000000 00000000
03: DID:000000 WWN:00000000 00000000
04: DID:000000 WWN:00000000 00000000
05: DID:000000 WWN:00000000 00000000
06: DID:000000 WWN:00000000 00000000
07: DID:000000 WWN:00000000 00000000
08: DID:000000 WWN:00000000 00000000
```

13 Wählen Sie [01: DID:0000000 WWN: 00000000 00000000], und drücken Sie [Enter].
Es wird das folgende Menü angezeigt:

```
      Selected Boot Device in Flash:
01: DID:000000 WWN:00000000 00000000 LUN: 0000

           1. Scan Targets
           2. Clear Flash Boot Info
```

14 Ziel suchen.
Wählen Sie [1. Scan Targets], und drücken Sie [Enter].
Es wird eine Datenliste wie im Folgenden gezeigt ausgegeben

```
Here are targets numbers 001 thru 001:

001: DID:0000EF WWN:202C00E0 00CB0815
```

15 Wählen Sie mit den Cursor-Tasten das gewünschte Ziel, und drücken Sie [Enter]. Die LUNs, die mit dem Ziel verbunden sind, werden wie im Folgenden gezeigt ausgegeben:

```
Here are Luns numbers 0001 thru 0001:

0001: Mode: Peripheral dev LUN: 0000
```

16 Wählen Sie die LUN, die für das Booten verwendet werden soll, und drücken Sie [Enter].

```
              Selected Boot Device:
001: DID:0000EF WWN:202C00E0 00CB0815 Mode: Per LUN: 0000

           1. Boot this device via WWN.
           2. Boot this device via DID.
```

17 Wählen Sie [1. Boot this device via WWN], und drücken Sie [Enter].
Es wird eine Liste wie die folgende angezeigt:

```
01: DID:000000 WWN:202C00E0 00CB0815 Mode: Per LUN: 0000
02: DID:000000 WWN:00000000 00000000
03: DID:000000 WWN:00000000 00000000
04: DID:000000 WWN:00000000 00000000
05: DID:000000 WWN:00000000 00000000
06: DID:000000 WWN:00000000 00000000
07: DID:000000 WWN:00000000 00000000
08: DID:000000 WWN:00000000 00000000
```

18 Drücken Sie die [Esc]-taste 5 Mal. Die Anzeige kehrt zurück zur EFI Shell.

```
 Drv[22]  Ctrl[ALL]  Lang[eng] - Options set.  Action Required is None
None

Shell>
```

19 Einstellungen aktivieren.
Führen Sie für die Partition einen Reset aus. Wählen Sie im [Power Control]-Fenster im [Power Control] Pull-Down Menü für die entsprechende Partition [Reset], und klicken Sie auf [Apply]. Alternativ können Sie das reset-Kommando verwenden.

```
 Shell> reset
```

Bem.: Weitere Einzelheiten finden Sie auf der EFIBoot Web Site der Emulex Corporation.
http://www.emulex.com/ts/index.jsp

D.4.4.2 EFI-Treiber (Version 3.11a4/ Version 3.11x1 konfigurieren)

1 Schalten Sie die Partition ein.
Auf der Konsole wird der [EFI Boot Manager] angezeigt.

```
EFI Boot Manager ver x.xx [x.xx]
Please select a boot option

    EFI Shell [Built-in]
    DVD/Acpi(PNP0A03,0)/Pci(1D|1)/Usb(0, 0)/Usb(1, 0)
    Network/Acpi(PNP0A03,0)/Pci(1E|0)/Pci(8|0)/Mac(000B5D6F80A9)
    Boot Option Maintenance Menu
    Setup Menu
```

2 Starten Sie die EFI-Shell.
Wählen Sie die Option [EFI Shell (Built-in)] und drücken Sie die [Enter]-Taste.
Die EFI-Shell wird gestartet.

3 Rufen Sie eine Liste der Treiber auf.
Geben Sie in der EFI-Shell folgendes Kommando ein und drücken Sie die [Enter]-Taste:

```
Shell> drivers -b
```

Eine Liste der Treiber ähnlich der nachfolgend dargestellten wird angezeigt. Suchen Sie nach dem Eintrag mit dem Text „Emulex SCSI Pass Thru Driver“ in der Spalte DRIVER NAME und notieren Sie den Wert, der in der Spalte DRV angezeigt wird. Im folgenden Beispiel ist die ID-Nummer des Treibers 22.

```
Shell> drivers -b
              T   D
D             Y C I
R             P F A
V   VERSION   E G G #D #C  DRIVER NAME                          IMAGE NAME
=== ======== = = = == === ============================== ==================
00D 00000010 B - -  2  43 PCI Bus Driver                       PciBus

020 00000010 B - -  3   3 USB Bus Driver                       UsbBus
021 00000010 D - -  1   - Usb Keyboard Driver                 UsbKeyboard
022 00031114 B X X  2   7 Emulex SCSI Pass Thru Driver        Elxcli311a4
Press ENTER to continue, 'q' to exit: q

Shell>
```

Hinweis: Die oben wiedergegebenen Informationen, einschließlich der ID-Nummern, variieren je nach der jeweiligen Umgebung.

4 List HBAs.

Geben Sie „drvcfg -s X“ ein, wobei X die im vorherigen Schritt 3 ermittelte ID-Nummer des Treibers ist, und drücken Sie die [Enter]-Taste. Eine Liste der installierten FC-Karten ähnlich der folgenden wird angezeigt.
Die Version des EFI-Treibers wird als EFI-Bios Utility und EFI Boot-Version ausgegeben.

```
                Emulex FC EFI-Bios Utility, Ver: 3.11a4
------------------------------------------------------------------
             Emulex Adapters in this System: 001 thru 002

001: LP11002         PCI-X  133MHz       Seg#: 00 Bus#: 49 Dev#: 01 Func#:
01
002: LP11002         PCI-X  133MHz       Seg#: 00 Bus#: 49 Dev#: 01 Func#:
00
```

Hinweis: Die Positionen der physikalischen Slots können entsprechend den im Fenster angezeigten Bus-Nummern und der Tabelle von PRIMEQUEST zu physikalischer Position - Bus-Nummer ermittelt werden. Stellen Sie sicher, dass sie übereinstimmen.
Die Tabelle von PRIMEQUEST zu physikalischer Position - Bus-Nummer finden Sie in Kapitel 4, „Physical Positions and Bus Numbers“, im Handbuch *Reference Manual: Tool/Operation Information* (C122-E074EN/ U41757-J-Z816-x-76).
PRIMEQUEST 580A/540A/580/540/480/440
→ „PRIMEQUEST 580A/540A/580/540/480/440 PCI Slot Physical Positions and Bus Numbers“
PRIMEQUEST 520A/520/420
→ „PRIMEQUEST 520A/520/420 PCI Slot Physical Positions and Bus Numbers“

5 Wählen Sie den HBA aus.

Setzen Sie den Cursor mit den Cursor-Tasten in der Liste der HBAs auf den Eintrag, der für die SAN Boot Environment benutzt werden soll, und drücken Sie die [Enter]-Taste. Es wird das Setup Utility-Menü angezeigt.

```
                Emulex FC EFI-Bios Utility, Ver: 3.11a4
------------------------------------------------------------------------
001: LP11002         PCI-X  133MHz       Seg#: 00 Bus#: 49 Dev#: 01 Func#: 01
             HBA Status: Ready             Boot Bios : Disabled
             EFI  Boot : BE3.11A4          Firmware  : BS2.10A7
------------------------------------------------------------------------
                             1. Setup Utility
                             2. Firmware Update
```

6 Anzeige des Menüs des HBA Setup Utilitys
Wählen Sie [1. Setup Utility] und drücken Sie [Enter]. Es wird das folgende Menü angezeigt.

```
              Emulex FC EFI-Bios Setup Utility, Ver: 3.11a4
------------------------------------------------------------------------
001: LP11002        PCI-X  133MHz      Seg#: 00 Bus#: 49 Dev#: 01 Func#:
01
         Boot Bios : Disabled  Firmware  : BS2.10A7  I/O Base  : 8200
         Port Name : 10000000C9537FB3  Node Name : 20000000C9537FB3
         S_ID      : 000000    Link Speed: NA        Topology  : Invalid
------------------------------------------------------------------------
                          1. Enable or Disable BIOS
                          2. Configure HBA Parameters
                          3. Configure Boot Parameters
                          4. Reset to Default Values
```

7 Ermitteln der WWPN des HBAs
Die WWPN des HBAs wird im menü (Schritt 6) als „Port Name“ angezeigt.

8 Aktivieren Sie die Einstellungen für den HBA.
Wählen Sie im Menü (Schritt 6) [4. Reset to Default Values].
Geben Sie in der erscheinenden Dialogbox „y“ ein.

```
Do you want to Force defaults (y/n) :
```

Hinweis: Unmittelbar nach Auslieferung des Systems ist dieser Schritt nicht erforderlich, da die Einstellung bereits erfolgt ist.

9 Aktivieren Sie die BIOS Boot Option.
Wählen Sie im Menü (Schritt 6) [1. Enable or Disable BIOS].
Es wird das folgende Menü angezeigt:

```
 EFI-Bios Boot Option is Currently DISABLED.
             Disabled - default
             Enabled
```

Wählen Sie [Enabled].

10 Drücken Sie einmal die [Esc]-Taste um zum Bildschirm von Schritt 6 zurückzukehren.

11 Geben Sie das Boot-Gerät an.
Wählen Sie im Menü (Schritt 6) [3. Configure Boot Parameters].
Es wird das folgende Menü angezeigt:

```
1. Device Path Selection
2. Maximum Luns/Target
3. Boot Target Scan
4. Configure Boot Devices
5. Delay Device Dicovery
```

12 Wählen Sie [4. Configure Boot Devices]. Es wir eine Datenliste wie im folgenden gezeigt ausgegeben. Wählen Sie einen leeren Eintrag. Bei Auslieferung des Sytems sind alle Einträge leer.

```
01: DID:000000 WWN:00000000 00000000
02: DID:000000 WWN:00000000 00000000
03: DID:000000 WWN:00000000 00000000
04: DID:000000 WWN:00000000 00000000
05: DID:000000 WWN:00000000 00000000
06: DID:000000 WWN:00000000 00000000
07: DID:000000 WWN:00000000 00000000
08: DID:000000 WWN:00000000 00000000
```

13 Wählen Sie [01: DID:0000000 WWN: 00000000 00000000], und drücken Sie [Enter].
Es wird das folgende Menü angezeigt:

```
      Selected Boot Device in Flash:
01: DID:000000 WWN:00000000 00000000 LUN: 0000

           1. Scan Targets
           2. Clear Flash Boot Info
```

14 Ziel suchen.
Wählen Sie [1. Scan Targets], und drücken Sie [Enter].
Es wir eine Datenliste wie im folgenden gezeigt ausgegeben

```
Here are targets numbers 001 thru 001:

001: DID:0000EF WWN:202C00E0 00CB0815
```

15 Wählen Sie mit den Cursor-Tasten das gewünschte Ziel, und drücken Sie [Enter]. Die LUNs, die mit dem Ziel verbunden sind, werden wie im folgenden gezeigt ausgegeben:

```
Here are Luns numbers 0001 thru 0001:

0001: Mode: Peripheral dev LUN: 0000
```

16 Wählen Sie die LUN, die für das Booten verwendet werden soll, und drücken Sie [Enter].

```
              Selected Boot Device:
001: DID:0000EF WWN:202C00E0 00CB0815 Mode: Per LUN: 0000

           1. Boot this device via WWN.
           2. Boot this device via DID.
```

17 Wählen Sie [1. Boot this device via WWN], und drücken Sie [Enter].
Es wird eine Liste wie die folgende angezeigt:

```
01: DID:000000 WWN:202C00E0 00CB0815 Mode: Per LUN: 0000
02: DID:000000 WWN:00000000 00000000
03: DID:000000 WWN:00000000 00000000
04: DID:000000 WWN:00000000 00000000
05: DID:000000 WWN:00000000 00000000
06: DID:000000 WWN:00000000 00000000
07: DID:000000 WWN:00000000 00000000
08: DID:000000 WWN:00000000 00000000
```

18 Drücken Sie die [Esc]-taste 5 Mal. Die Anzeige kehrt zurück zur EFI Shell.

```
 Drv[22]  Ctrl[ALL]  Lang[eng] - Options set.  Action Required is None
None

Shell>
```

19 Einstellungen aktivieren.
Führen Sie für die Partition einen Reset aus. Wählen Sie im [Power Control]-Fenster im [Power Control] Pull-Down Menü für die entsprechende Partition [Reset], und klicken Sie auf [Apply]. Alternativ können Sie das reset-Kommando verwenden.

```
 Shell> reset
```

Bem.: Weitere Einzelheiten finden Sie auf der EFIBoot Web Site der Emulex Corporation.
http://www.emulex.com/ts/index.jsp

D.4.5 Hinweise zum Austausch eine FC-Karte

Gehen Sie wie in Appendix D.4.4 „EFI-Treiber konfigurieren“ beschrieben vor, um das Boot Device für die neue FC-Karte einzustellen, wenn das Boot Device an die ausgetauschte Karte angeschlossen war.

Nehmen Sie ebenfalls die für den angeschlossenen FC Switch und die angeschlossenen Speichereinheiten erforderlichen Einstellungen vor, wie in den zugehörigen Handbüchern beschrieben.

- Ändern Sie die Zone-Einstellung für den FC-Switch (bei der Einstellung der WWN Zone).
- Ändern Sie die ETERNUS* Host-Affinity Einstellung.
- Ändern Sie die EFI-Treibereinstellung.

*: Angebot und Support in EMEA nur für die globalen Kunden von Fujitsu

D.5 Installation des Betriebssystems

Die Installation des Betriebssystems ist in Abschnitt 3.3, „Windows installieren“ beschrieben.

Anm.:

- Installieren Sie das Betriebssystem so, dass nur die LUN, auf der es installier wird, identifiziert werden kann.
- Installieren Sie das Betriebssystem in einer 1-Pfad-Umgebung.
- Hängen Sie das interne SCSI-Laufwerk aus, bevor Sie das Betriebssystem installieren.
  Hängen Sie das SCSI-Laufwerk wieder in ihre IO Unit ein, wenn die Installation des Betriebssystems abgeschlossen ist.
- Wenn das Betriebssystems installiert ist, fahren Sie mit der Installation von ETERNUS* MPD fort. Folgen Sie dabei den Anweisungen im ETERNUS* MPD Handbuch. ETERNUS* MPD wird erst nach Starten des Betriebssystems erkannt.

Hinweis: Die folgende Meldung wird angezeigt, wenn die Taste [F6] gedrückt wird, um die FC-Treiber zu installieren. Verbinden Sie gemäß den angezeigten Anweisungen das USB-Diskettenlaufwerk an die USB-Port der KVM-Einheit und drücken Sie die [S]-Taste. Schließen Sie das USB-Diskettenlaufwerk nicht an den USB-Port der IO Unit an.

```
Setup could not determine the type of one or more mass storage devices
     installed in your system, or you have chosen to manually specify an adapter.
     Currently, Setup will load support for the following mass storage device(s):

     <none>

     * To specify additional SCSI adapters, CD-ROM drivers, or special
       disk controllers for use with Windows, including those for
       which you have a device support disk from a mass storage device
       manufacturer, press S.

     * If you do not have any device support disks from a mass storage
       device manufacturer, or do not want to specify additional mass
       storage devices for use with Windows, press ENTER.
```

*: Angebot und Support in EMEA nur für die globalen Kunden von Fujitsu

Pfadänderung bei Systemstart

Der Booteintrag für Windows Server 2003 für Itanium-basierte Systeme beruht auf einer GUID (Globally Unique Identifier). Wenn es also zu einem Fehler in dem Pfad vom FC-Switch zum SAN-Speicher kommt, kann das Betriebssystem gestartet werden, vorausgesetzt das Boot-Gerät ist über einen anderen Pfad erreichbar.

Anhang E Liste der Standardwerte

Die folgende Tabelle enthält Informationen, die im Problemfall hilfreich sein können, sowie einen Überblick über die Standardwerte für Einstellungen.

E.1 Default-Werte für MMB

Tabelle E.1 Liste der möglichen Werte für MMB

Fenster	Übergeordn. Kategorie	Untergeordn. Kategorie	Einstellung	Default-Wert	Mögliche Werte	Bemerkungen
System Event Log Filter Button	Setting of event log filtering conditions	Selection of severity for display	Severity	Alle aktiviert	• Error • Warning • Info • Monitor * Mehrere Positionen können ausgewählt werden.	
		Selection of partition to be displayed	Partition	Alle Optionsfelder	• All • Specified	Beim Wechsel zwischen „All“ und „Specified“ bleibt die Auswahl unter „Specified“ erhalten.
		Selection of target source for display	Source	Alle	• All • Specified	Beim Wechsel zwischen „All“ und „Specified“ bleibt die Auswahl unter „Specified“ erhalten.
		Selection of target unit for display	Unit	Alle	• All • Specified	Beim Wechsel zwischen „All“ und „Specified“ bleibt die Auswahl unter „Specified“ erhalten.
		Specification of display order	Sort by Date/ Time	Neuer Vorgang zuerst	• Neuer Vorgang zuerst • Alter Vorgang zuerst	

Tabelle E.1 Liste der möglichen Werte für MMB

Fenster	Übergeordn. Kategorie	Untergeordn. Kategorie	Einstellung	Default-Wert	Mögliche Werte	Bemerkungen
System Event Log Filter Button	Setting of event log filtering conditions	Selection of whether to begin event output with the first event or specify the time	Start Date/ Time	First Event	• First event • Specified Time	Bei Auswahl von „Time“ kann ein Startzeitpunkt definiert werden. Bei Wechsel zu „First Event“ wird die Zeitangabe beibehalten.
		Selection of whether to end event log output with the last event or specify the time	End Date/ Time	End Event	• End event • Specified Time	Bei Auswahl von „Time“ kann ein Startzeitpunkt definiert werden. Bei Wechsel zu „Last Event“ wird die Zeitangabe beibehalten.
		Specification of the number of log events to be displayed	Number of events to display	100 events	Ganzzahl größer oder gleich 0 und kleiner als der Nenner des angezeigten Bruchs	Der Nenner des angezeigten Bruchs ist die Gesamtzahl der Ereignisse in der Logdatei.
System Information	System name setting	Setting PRIMEQUEST system name	System Name	PRIMEQUEST + Serien-Nr. des Rechners	Max. 64 Zeichen.	Dient auch als SNMP-Rechnername
	Asset tag information setting	Asset management information setting	Asset Tag	None	Bis zu 32 Zeichen können eingegeben werden.	
System Setup	Power-related setting	Setting power for PRIMEQUEST system	Power Feed Mode	Single	• Single (single power feed mode) • Dual (dual power feed mode)	
		Setting procedure for power recovery	Power Restore Policy	Restore	• Always OFF • Always ON • Restore	
		Setting procedure when redundancy is lost	Power Fault Reaction	Continue	• Continue • Shutdown	
		Setting delay time till OS shutdown begins after UPS detects AC Lost	Shutdown Delay after UPS detects AC Lost	5 Sek.	0 bis 9999 Sek.	

Tabelle E.1 Liste der möglichen Werte für MMB

Fenster	Übergeordn. Kategorie	Untergeordn. Kategorie	Einstellung	Default-Wert	Mögliche Werte	Bemerkungen
System Setup	Setting of GSWB OFF at shutdown (nur PRIMEQUEST 580A/540A*/ 580/540/480/ 440)	Setting to synchronically turn off the power to the cabinet and GSWB	Power Linkage Mode	Aktiviert (Schrank und GSWB werden gleichzeitig ausgeschaltet.)	Aktiviert: Wenn alle Partitionen heruntergefahren werden, wird auch die Stromversorgung zum Schrank und GSWB abgeschaltet. Deaktiviert: Selbst wenn alle Partitionen heruntergefahren werden, wird der Schrank und das GSWB nicht mit ausgeschaltet.	
	Setting of mounting altitude	Setting mounting altitude	Altitude	Altitude <= 1500m	• Altitude <= 1500m • 1500m < Altitude <= 2000m • 2000m < Altitude <= 2500m • 2500m < Altitude	
	Setting of Mirror Mode	Setting Mirror Mode	Mirror Mode (setting)	Aktiviert	• Enable (Mirror Mode aktiviert) • Disable (Mirror Mode nicht aktiviert)	Das Chassis muss ausgeschaltet werden, damit die Änderung in Kraft tritt. Nehmen Sie daher die Einstellung im System vor, bevor das Chassis ausgeschaltet wird.
System Power Control	Cabinet power ON/OFF control	Power control of PRIMEQUEST system	System Power Control	Keine	• Power On - alle angegebenen Partitionen werden eingeschaltet. • Power On chassis only (*) • Power Off - das Chassis wird ausgeschaltet, nachdem alle Partitionen heruntergefahren wurden. • Force Power Off	Keine Voreinstellung * Nur bei PRIMEQUEST 580A/540A*/580/ 540/480/440.
Power Control	Partition power control	Setting forced power-off	Force Power Off Delay	Keine Voreinstellung	Wenn „Forced Power-off“ aktiviert ist, kann eine Verzögerung angegeben werden (1 bis 9 Minuten).	Die Partition wird nach Ablauf der definierten Zeitdauer ausgeschaltet.
Schedule Control	Partition scheduled-operation setting	Power-on/off setting for each partition	Schedule Control		• On • Off	

Tabelle E.1 Liste der möglichen Werte für MMB

Fenster	Übergeordn. Kategorie	Untergeordn. Kategorie	Einstellung	Default-Wert	Mögliche Werte	Bemerkungen
Schedule List	Schedule setting	Setting power-on/off schedule of each partition	Schedule List	Keine	Zeitplan für jede Partition festlegen. 1 Daily: Partitionen tägliche ein-/ausschalten. Zeitpunkt angeben. 2 Weekly: Partitionen wöchentlich ein-/ausschalten. Wochentag und Start- und Endedatum festlegen. 3 Monthly: Partitionen monatlich ein-/ausschalten. Dauer (Start- und Endezeitpunkt) angeben. 4 Special: Partitionen an spez. Tag ein-/ausschalten. Datum angeben. Soll die Partition am definierten Tag ein- oder ausgeschaltet werden? Uhrzeit angeben. Minuten in 10er Schritten angeben (00, 10, 20, 30, 40, or 50).	Mit der Schaltfläche Add erstellen Sie einen Zeitplan. Ansonsten wählen Sie einen bereits bestehenden Zeitplan aus und editieren ihn (Schaltfläche Edit) oder löschen ihn (Schaltfläche Remove).
Console Redirection Switch	Console Redirection Switch	Setting OS serial output destination	Connect to	COM	• COM • MMB	
		Setting console redirection port number	Port	Keine	Port-Nr. 1024 oder höher.	
		Setting console redirection connection protocol (Telnet/SSH)	Telnet/SSH	Telnet	• Telnet • SSH • None	Diese Option ist aktiviert, wenn MMB bei „Connect to“ ausgewählt wurde. Bei „None“ wird nur die Seite [WebUI Console Redirection] angezeigt.
Partition Configuration	Partition setting	Setting partition name	Partition Name	NULL	Max. 16 Zeichen	Leicht zu erkennen, wenn der im Betriebssystem definierte Hostname verwendet wird.

Tabelle E.1 Liste der möglichen Werte für MMB

Fenster	Übergeordn. Kategorie	Untergeordn. Kategorie	Einstellung	Default-Wert	Mögliche Werte	Bemerkungen
Home of Partition	Selection of home IOU	Setting home IOU	Home IOU	Keine	IO Unit der Partition, d.h. IO Unit mit BMM	
Reserved SB Configuration	Setting of reserved SB	Setting reserved SB	Reserved SB Configuration	Keine	Freies Systemboard, bzw. bereits als für eine Partition reserviertes Systemboard.	
Boot Control	Specification of boot device	Specification of boot device	Boot Selector	No Override	• No Override • Force boot into EFI Boot Manager • Force PXE • Force boot from DVD	
	Setting of POST (Power On Self Test)	Setting POST (Power On Self Test)	POST	• Standard Diagnosis	• Fast Boot • Standard Diagnosis • Full Diagnosis	
ASR Control	ASR Control setting	Setting the number of retries involving the OS restart	Number of Restart Tries	5	0 bis 10	
		Setting remedial action when the specified retry count is exceeded	Action after exceeding Restart tries	Stop rebooting and Power Off	• Stop rebooting and Power Off • Stop rebooting • Diagnostic Interrupt assert	
		Setting the power-on delay time for automatic rebooting	Automatic Power On Delay	0	0 bis 10	
		Canceling OS boot monitoring	Cancel Boot Watchdog	No check	Check: Boot Watchdog cancel	
System Power Control	Registration of Virtual Floppy image	Registration of Virtual Floppy image	Registration of floppy image	Keine	Register a floppy image	

Tabelle E.1 Liste der möglichen Werte für MMB

Fenster	Übergeordn. Kategorie	Untergeordn. Kategorie	Einstellung	Default-Wert	Mögliche Werte	Bemerkungen
Mode	Setting various types of mode	Setting Partition PCI Address Mode (nur PRIMEQUEST 580A/540A*/ 580/540/480/ 440)	PCI Address Mode (setting)	PCI Bus Mode	• PCI Bus Mode • PCI Segment Mode	
		Setting Mirror Mode	Mirror Mode (setting)	Standard Mirror Mode	• Standard Mirror Mode • Extended Mirror Mode	Modus tritt nach Neustart der Partition in Kraft. Wenn die PRIMEQUEST im Non-Mirror-Modus läuft, steht Mirror Mode hier nicht zur Verfügung.
		Hyper Threading	Hyper Threading (setting)	Disable	• Enable • Disable	
		Dynamic Partitioning	Dynamic Partitioning (setting)	Disable	• Enable • Disable	

Tabelle E.1 Liste der möglichen Werte für MMB

Fenster	Übergeordn. Kategorie	Untergeordn. Kategorie	Einstellung	Default-Wert	Mögliche Werte	Bemerkungen
Add/Edit User	Setting user account	Setting user name	User name	Keine	8 bis 32 Zeichen. Folgende Zeichen sind erlaubt: 0 bis 9, a bis z, A bis Z, - und _. Das erste Zeichen muss ein Buchstabe sein.	
		Setting password	Password	Keine	Geben Sie ein Kennwort aus 8 bis 32 Zeichen ein. Es darf nicht zu einfach zu erraten sein. Wenn das Kennwort nicht gültig ist, wird die Eingabe eines anderen Kennworts gefordert. Folgende Zeichen sind erlaubt: Ziffern 0 bis 9 Buchstaben: a bis z und A bis Z Sonderzeichen: ! " # $ % & ' ( ) = - ^ ~ \ @ `[ ] { } : * ; + ? < .>, / _ |	
		Setting user account privileges	Privilege	Admin (Add User)/current Privilege (Edit User)	• Admin • Operator • User • CE	
		Enable/disable the use of user account	Status	Enable (Add User)/current Status (Edit User)	• Enabled • Disabled	

Tabelle E.1 Liste der möglichen Werte für MMB

Fenster	Übergeordn. Kategorie	Untergeordn. Kategorie	Einstellung	Default-Wert	Mögliche Werte	Bemerkungen
Date/Time	Definition of MMB date/time adjustment	Date setting	Date	Keine	Datum	
		Setting hour:minute:second	Display hour:minute:second (24-hour format)	Keine	Stunde:Min:Sek (24-Std-Format)	
		Timezone setting	Time zone	Keine	Aus Dropdown-Liste auswählen.	
		Enable/disable NTP function	NTP enable/ disable	Disable	• Enable • Disable	
		Setting IP address of primary NTP server	NTP 1	Keine	0 bis 255, 0 bis 255, 0 bis 255, 0 bis 255	
		Setting IP address of secondary NTP server	NTP 2	Keine	0 bis 255, 0 bis 255, 0 bis 255, 0 bis 255	
		Setting IP address of third NTP server	NTP 3	Keine	0 bis 255, 0 bis 255, 0 bis 255, 0 bis 255	
Network Interface	Setting system network	Setting virtual IP address (PRIMEQUEST 580A/540A*/ 580/540/480/ 440)	Virtual IP Address		Virtuelle IP-Adresse für Zugriff auf Web-UI angeben.	
		Setting MMB IP address (PRIMEQUEST 520A*/520/420)	IP Address		physikalische IP-Adresse des MMB angeben.	
		Setting MMB#0 IP address (PRIMEQUEST 580/540/480/ 440)	MMB#0 IP Address		physikalische IP-Adresse von MMB 0 angeben.	
		Setting MMB#1 IP address (PRIMEQUEST 580A/540A*/ 580/540/480/ 440)	MMB#1 IP Address		physikalische IP-Adresse von MMB 1 angeben.	
		Specification of whether to use a DNS server	DNS	Disable	• Enable • Disable	

Tabelle E.1 Liste der möglichen Werte für MMB

Fenster	Übergeordn. Kategorie	Untergeordn. Kategorie	Einstellung	Default-Wert	Mögliche Werte	Bemerkungen
Management LAN Port Configuration	Setting management LAN	Setting MMB HUB VLAN mode	VLAN Mode	VLAN mode	• No VLAN mode • VLAN mode • Port disable mode	
		Setting MMB#0 Port Speed/ Duplex (PRIMEQUEST 580A/540A*/ 580/540/480/ 440)	Speed/Duplex for MMB#0	Auto	• Auto • 100M/Full • 100M/Half • 10M/Full • 10M/Half	Ausgegraut, wenn MMB 0 nicht eingehängt ist.
		Setting MMB#1 Port Speed/ Duplex (PRIMEQUEST 580A/540A*/ 580/540/480/ 440)	Speed/Duplex for MMB#1	Auto	• Auto • 100M/Full • 100M/Half • 10M/Full • 10M/alf	Ausgegraut, wenn MMB 1 nicht eingehängt ist.
		Setting MMB Port Speed/Duplex (PRIMEQUEST 520A/520/420)	Speed/ Duplex for MMB	Auto	• Auto • 100M/Full • 100M/Half • 10M/Full • 10M/Half	
Network Protocols	HTTP/HTTPS setting	HTTP setting	HTTP	Disable	• Enable • Disable	
		Setting HTTP Port Number	HTTP Port#	8081	1024 bis 65535	
		Enable/disable HTTPS	HTTPS	Disable	• Enable • Disable	
		Setting HTTPS Port Number	HTTPS Port#	432	432,1024 bis 65535	
		Setting HTTP/ HTTPS connection timeout	HTTP/ HTTPS Timeout	600 s	0,60-9999 s	
	Telnet setting	Enable/disable telnet	Telnet	Disable	• Enable • Disable	
		Setting the port used for telnet	Telnet port	23	23,1024 bis 65535	
		Setting telnet connection timeout	Telnet Timeout	600 s	0,60-9999 s	
	SSH setting	Enable/disable SSH	SSH	Disable	• Enable • Disable	
		Setting SSH port	SSH port	22	22,1024 bis 65535	
		Setting SSH connection timeout	SSH Timeout	600 s	0,60-9999 s	

Tabelle E.1 Liste der möglichen Werte für MMB

Fenster	Übergeordn. Kategorie	Untergeordn. Kategorie	Einstellung	Default-Wert	Mögliche Werte	Bemerkungen
Network Protocols	SNMP setting	Enable/disable SNMP Agent	SNMP Agent	Disable	• Enable • Disable	
		Setting the port used for SNMP Agent	SNMP Agent port	161	161, 1024 bis 65535	
		Enable/disable SNMP Trap	SNMP Trap	Disable	• Enable • Disable	
		Setting the port used for SNMP Trap	SNMP Trap port	162	162, 1024 bis 65535	
Refresh Rate	Setting automatic refresh of WebUI	Setting refresh	Refresh Rate	Auto-Refresh = Disable	5 bis 999 s	
SNMP Community	Setting system SNMP	Setting SNMP System Location	System Location	Keine	Zeichenkette	
		Setting SNMP System Contact	SNMP System Contact	Keine	Zeichenkette	
		Setting SNMP community string	Community/ User	Keine	Zeichenkette	
		Setting access-enabled IP Address or subnet	IP Address/ MASK	Keine	0 bis 255, 0 bis 255, 0 bis 255, 0 bis 255	
		Setting SNMP Version	SNMP Version	Read Only	• 1 • 2 • 3	
		Enable read only or read/ write	Access	Keine	• Read Only • Read Write	
		Setting security level	Auth	Keine	• noauth • auth • priv	

Tabelle E.1 Liste der möglichen Werte für MMB

Fenster	Übergeordn. Kategorie	Untergeordn. Kategorie	Einstellung	Default-Wert	Mögliche Werte	Bemerkungen
Create CSR	Creation of SSL certificate	Length of private key (bits)	Key length	1024	• 1024 • 2048	
		ISO country code of owner	Country Name	Keine	• Japan: JP • USA: US	
		State or province of owner	State or Province Name	Keine	Max. 56 Zeichen	
		Owner locality name	Locality Name	Keine	Max. 56 Zeichen	
		Owner organization name (company name)	Organization Name	Keine	Max. 56 Zeichen	
		Owner organization unit name	Organization Unit Name	Keine	Max. 56 Zeichen	
		Owner server FQDN	Common Name	Keine	Max. 56 Zeichen	
		Email address	Email Address	Keine	Max. 40 Zeichen	
Create Selfsigned Certificate	Creation of SSL certificate	Term of self-signing certificate validity	Term	Keine	Anzahl Tage	
		Length of private key (bits)	Key length	1024	• 1024 • 2048	
		ISO country code of owner	Country Name	Keine	• Japan: JP • USA: US	
		State or province of owner	State or Province Name	Keine	Max. 56 Zeichen	
		Owner locality name	Locality Name	Keine	Max. 56 Zeichen	
		Owner organization name (company name)	Organization Name	Keine	Max. 56 Zeichen	
		Owner organization unit name	Organization Unit Name	Keine	Max. 56 Zeichen	
		Owner server FQDN	Common Name	Keine	Max. 56 Zeichen	
		Email address	Email Address	Keine	Max. 40 Zeichen	

Tabelle E.1 Liste der möglichen Werte für MMB

Fenster	Übergeordn. Kategorie	Untergeordn. Kategorie	Einstellung	Default-Wert	Mögliche Werte	Bemerkungen
SNMP Trap	SNMP trap-send destination setting	System or user name setting	Community/ User	None		
		IP address setting of the trap-send destination	IP Address	None	0 to 255, 0 to 255, 0 to 255, 0 to 255	
		SNMP version setting	SNMP Version	None	• 1 • 2 • 3	
		Security level setting	Auth	None	• noauth • auth • priv	
		Hash function setting	Auth Type	None	• MD5 • SHA	Valid only for SNMP version 3
Edit User	User setting required for MMB control with RMCP	Setting user name	User name	user 0 to user 23	8 bis 16	Nur „en-sized“ alphabetische Zeichen (Groß- und Kleinbuchstaben) und „en-sized“ numerische Zeichen sind erlaubt
		Password setting	Password	None	8 bis 16	Nur „en-sized“ alphabetische Zeichen (Groß- und Kleinbuchstaben) und „en-sized“ numerische Zeichen sind erlaubt
		Setting user account privileges	Privilege	No Access	• Admin • Operator • User • CE • No Access	Benutzer mit „No Access“ hat keinen entfernten Zugriff auf das System.
		Setting for enabling or disabling a user account	Status	Disabled	• Enabled • Disabled	
Access Control	Access control setting for the network protocol to ensure MMB security	Subnet mask of an IP address that can be used for connection	Subnet Mask	None	0 bis 255	Beispiel: 255.255.255.0

Tabelle E.1 Liste der möglichen Werte für MMB

Fenster	Übergeordn. Kategorie	Untergeordn. Kategorie	Einstellung	Default-Wert	Mögliche Werte	Bemerkungen
Add/Edit Filter	Definition of MMB IP Filtering	Setting IP Filtering	Protocol	SSH	• HTTP • HTTPS • Telnet • SSH • SNMP	
		Enable/disable Access Control	Access Control	Disable	• Enable • Disable	
		IP address enabled for connection	IP Address	None	0 to 255, 0 to 255, 0 to 255, 0 to 255	Example: 192.168.0.0
		Subnet Mask of IP Address enabled for connection	Subnet Mask	None	0 to 255, 0 to 255, 0 to 255, 0 to 255	Example: 255.255.255.0
Alarm E-Mail	Setting e-mail address for event occurrence notification	Setting alarm email	Alarm Email	Disable	• Enable • Disable	
		Setting sender email address	From:	Keine	Email-Adresse	
		Setting recipient email address	To:	Keine	Email-Adresse	
		Setting SMTP server IP address or FQDN	SMTP Server	Keine	IP-Adresse oder FQDN des SMTP-Servers	FQDN nur verfügbar, wenn DNS gesetzt ist.
		Setting mail subject	Subject	Keine	Zeichenkette	
Alarm E-Mail Filter Button	Setting of notification destination (e-mail) in predictive monitoring	Selection of display severity check box	Severity	All check boxes	• Error • Warning • Info * Mehrere Optionen möglich.	
		Selection of display partition check box	Partition	All check boxes	Partition(en) auswählen. * Mehrere Optionen möglich.	
		Selection of display target unit	Unit	All	Anzuzeigende Einheit auswählen.	
		Selection of display target unit	Source	All	Anzuzeigende Quelle auswählen.	
Custom TimeZone	Setting a custom time zone	Setting a custom time zone	Custom TimeZone	Keine	Zeitzone	
SNMP v3 Configuration	Setting of system SNMPV3	Setting Engine ID specific to SNMP v3	SNMP v3 Configuration	Engine ID: None User Name: None Auth Type: MD5 Authpassphrase / Privpassphrase: None	EngineID für SNMP V.3	

Tabelle E.1 Liste der möglichen Werte für MMB

Fenster	Übergeordn. Kategorie	Untergeordn. Kategorie	Einstellung	Default-Wert	Mögliche Werte	Bemerkungen
Mode License	Setting of mirror license	Setting system mirror	System Mirror	Keine	System Mirror-Lizenz	
XPAR License	XPAR license setting	XPAR setting	License	Keine	Lizenz für Aktivierung von XPAR	
32CPU License(PRIMEQUEST 580A/ 540A*/580/ 540)	32-CPU license setting	Setting for enabling operation as a 32-CPU system	License	Keine	Lizenz für Aktivierung des 32-CPU-Systembetriebs.	
32CPU License (PRIMEQUEST 480/440)	32-CPU license setting	Setting for enabling operation as a 32-CPU system	License	None	Lizenz für Aktivierung des 32-CPU-Systembetriebs.	

*: wird von Fujitsu Technology Solutions nicht unterstützt

E.2 Werte für PSA eingeben

Tabelle E.2 Liste der möglichen Werte für PSA

Übergeord. Kategorie	Untergeord. Kategorie	Einstellung	Default-Wert	Mögliche Werte	Anmerkung
Process List	Process list	Refresh Time	Keine	• None • 5 sec • 10 sec • 30 sec • 60 sec	
		Signal	SIGTERM	• SIGTERM • SIGHUP • SIGKILL • SIGINT • SIGQUIT	
S.M.A.R.T. setting		S.M.A.R.T. Monitoring	Enable	• Enable • Disable	
Watchdog setting	Software Watchdog setting	Watchdog	Disable	• Enable • Disable	
		TimeOut	3600 (sec)	60 bis 6000 (Sek.)	Angabe nur bei „Enable“ möglich.
		Watchdog Action	No Action	• No Action • Reset • Power Off • Power Cycle/INIT	Angabe nur bei „Enable“ möglich.
	Boot Watchdog setting	Watchdog	Disable	• Enable • Disable	
		TimeOut	0 (sec)	60 bis 6000 (Sek.)	Angabe nur bei „Enable“ möglich. Default-Wert nicht übernehmbar.

Tabelle E.2 Liste der möglichen Werte für PSA

Übergeord. Kategorie	Untergeord. Kategorie	Einstellung	Default-Wert	Mögliche Werte	Anmerkung
AgentLog	AgentLog condition specification	Severity	Error/Warning/ Information (all)	• Error • Warning • Information * Mehrere Optionen möglich.	
		Unit	All	• All • SB • CPU • DIMM • IOU (IOU/IOX für PRIMEQUEST 420/ 520) • PCI_Card • Disk • Software • MMB/BMC • Network * Mehrere Optionen möglich. • Enter the Unit name directly	
		Sort by Date/ Time	New event first	• New event first • Old event first	
		Start Date/Time	First event	• First event • Specified Time	
		End Date/Time	End event	• End event • Specified Time	
		Number of events to display	1000	• 100 • 200 • 300 • 400 • 500 • 1000	
Export List	Export list	Select File	Top file (latest)	Herunterzuladende bzw. zu löschende Datei * Nur eine Auswahl möglich.	
	Export indication	Keyword	Blank	Max. 50 alphanum. Zeichen, Leerzeichen und/oder Sonderzeichen, außer <>%&”,\	

Anhang F Übersicht der IP-Adressen des Management-LANs

Das Management-LAN der PRIMEQUEST verwendet die in Abbildung F.1 und Abbildung F.2 angegebenen IP-Adressen.

PRIMEQUEST 580A/540A*/580/540/480/440

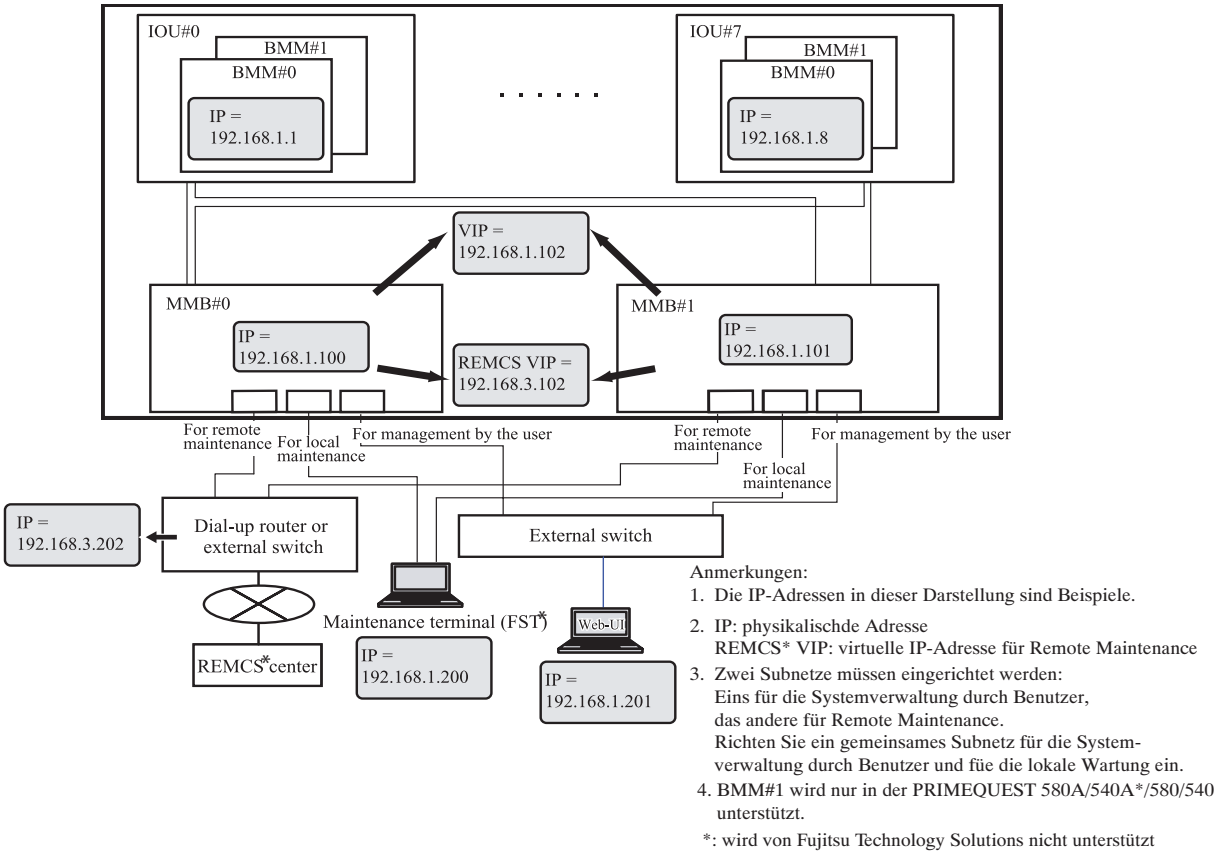


Abbildung F.1 Netzwerkkonfiguration und IP-Adressen des Management-LANs (PRIMEQUEST 580A/540A*/580/540/480/440)

Die wichtigsten verwendeten IP-Adressen werden im Folgenden beschrieben.

*: wird von Fujitsu Technology Solutions nicht unterstützt

- IP-Adressen des MMB

  Das MMB 0 und MMB 1 verfügen jeweils über eine physikalische IP-Adresse. Darüber hinaus können für beide MMBs eine virtuelle IP-Adresse sowie eine weitere virtuelle IP-Adresse für einen REMOTE MAINTENANCE-Anschluss festgelegt werden. Für eine Verbindung zu PRIMECLUSTER und Systemwalker wird die physikalische IP-Adresse verwendet.

  Die virtuelle IP-Adresse wird für den SNMP-Zugriff vom Managementserver oder von der MMB Web-UI benutzt. GSWB- und PSA-Operationen werden ebenfalls über die MMB Web-UI durchgeführt.

- Vom Betriebssystem einer Partition eingestellte IP-Adresse

  Dem auf einer Partition ablaufenden Betriebssystem muss eine IP-Adresse zugewiesen werden. physikalisch muss sich diese auf den NICs der IOU#0 bis IOU#7 befinden.

  Über diese IP-Adressen werden Web-UI-, SNMP- und REMCS*-Verbinungen zwischen dem PSA und dem MMB bzw. zwischen PRIMECLUSTER und dem MMB geleitet.

  Die BMMs der IO Units verfügen jeweils über zwei Netzwerkschnittstellen, die durch den Linux Bonding Driver oder PRIMECLUSTER GLS für Linux und durch das Teaming von Intel PROset für Windows redundant gemacht werden.

  Hinweis:

  - Wenn Sie als externen Schalter ein Switching Hub benutzen wollen, das einen Schleifenschutz (Spanning Tree Protocol oder Domain Separation) unterstützt, unterdrücken Sie den Schleifenschutz, indem Sie die Option [Spanning Tree Protocol] für den Port für die Verbindung zwischen dem Switching Hub und der Systemeinheit deaktivieren oder [Domain Separation] aktivieren.
  - Zur Kommunikation überträgt das MMB Pakete folgender Typen: NTP, Alarm-E-Mail, REMCS* und SNMP-Trap. Falls für das MMB sowohl eine physikalische IP-Adresse als auch eine virtuelle IP-Adresse eingestellt ist, wird die physikalische IP-Adresse als Absenderadresse verwendet.

*: wird von Fujitsu Technology Solutions nicht unterstützt

Unter den folgenden Bedingungen müssen Firewall, Mail und andere Dienste auf Durchlass der Pakete von MMB#0 und MMB#1 eingestellt werden:

- Ziel ist ein externes System außerhalb der Firewall.
- Die IP-Adressen werden vom verwendeten Mail-Server umgeleitet.

Falls darüber hinaus unter diesen Bedingungen der REMOTE MAINTENANCE-Port bei der PRIMEQUEST 580A/540A* verwendet wird, muss ebenfalls für die REMOTE MAINTENANCE-Pakete der Durchlass konfiguriert werden.

PRIMEQUEST 520A*/520/420

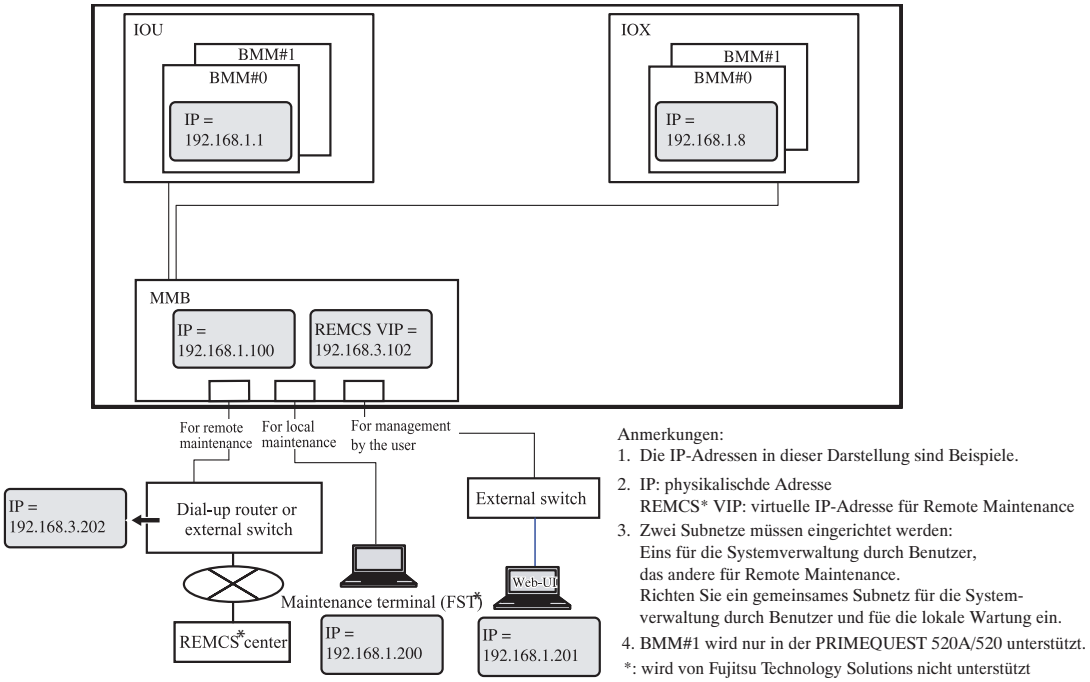


Abbildung F.2 Netzwerkkonfiguration und IP-Adressen des Management-LANs (PRIMEQUEST 52A*/520/420)

Die wichtigsten verwendeten IP-Adressen werden im Folgenden beschrieben.

- IP-Adressen des MMB

  Das MMB verfügt über eine IP-Adresse für das Management-LAN und eine virtuelle IP-Adresse für REMOTE MAINTENANCE.

*: wird von Fujitsu Technology Solutions nicht unterstützt

Die IP-Adresse für das Management-LAN wird vom Management-Server oder vom MMB Web-UI als SNMP-Zugangsziel benutzt. PSA-Operationen werden ebenfalls über das MMB Web-UI ausgeführt.

Hinweis:

- Wenn Sie als externen Schalter ein Switching Hub benutzen wollen, das einen Schleifenschutz (Spanning Tree Protocol oder Domain Separation) unterstützt, unterdrücken Sie den Schleifenschutz, indem Sie die Option [Spanning Tree Protocol] für den Port für die Verbindung zwischen den Switching Hub und der Systemeinheit deaktivieren oder [Domain Separation] aktivieren.
- Zur Kommunikation überträgt das MMB Pakete folgender Typen: NTP, Alarm-E-Mail, REMCS* und SNMP-Trap. Falls für das MMB sowohl eine physikalische IP-Adresse als auch eine virtuelle IP-Adresse eingestellt ist, wird die physikalische IP-Adresse als Absenderadresse verwendet.
  Unter den folgenden Bedingungen müssen Firewall, Mail und andere Dienste auf Durchlass der Pakete von MMB#0 und MMB#1 eingestellt werden:
  - Ziel ist ein externes System außerhalb der Firewall.
  - Die IP-Adressen werden vom verwendeten Mail-Server umgeleitet.

Falls darüber hinaus unter diesen Bedingungen der REMOTE MAINTENANCE-Port bei der PRIMEQUEST 520A* verwendet wird, muss ebenfalls für die REMOTE MAINTENANCE-Pakete der Durchlass konfiguriert werden

*: wird von Fujitsu Technology Solutions nicht unterstützt

Glossar

API

Abkürzung für Application Programming Interface. Eine gemeinsame Schnittstelle zur Entwicklung von Betriebssystemen und Middleware.

ASIC

Abkürzung für Application Specific Integrated Circuit. Ein für eine spezifische Anwendung entwickelter integrierter Schaltkreis.

Backplane

Das Backplane ist mit Systemboards, IO Units und sonstigen Geräten verbunden. Gemeinsam mit dem XAI und dem XDI bildet es die Verbindung zwischen Speicher- und IO Units (Crossbar).

BIOS

Abkürzung für Basic Input Output System. Das BIOS steuert als Bestandteil des Betriebssystems den Datenstrom zwischen einzelnen Systemkomponenten. Bei den Rechnern der PRIMEQUEST Familie wird BIOS als Überbegriff für PAL, SAL und EFI benutzt.

BMC

Abkürzung für Baseboard Management Controller. Der BMC benachrichtigt das Betriebssystem vom Auftreten schwerwiegender Hardwarefehler.

BMM

Abkürzung für BMC Module. Auf dem BMM befinden sich Legacy-Ein-/Ausgabeports, z.B. BMC, VGA, USB und COM-Ports.

Business-LAN

LAN, auf dem eine Anwendung konfiguriert ist.

CLI

Abkürzung für Command Line Interface. Diese Schnittstelle erlaubt eine direkte Ausführung von Kommandos auf der UNIX- oder DOS-Betriebssystemebene.

CoA

Abkürzung für Certificate of Authenticity. Dies ist ein sichtbares Erkennungszeichen für authentische Microsoft-Software und -Komponenten.

COM-Port (Communication Port)

Serielle RS-232C-Schnittstelle für PC/AT-kompatible Systeme. (Das COM-Port wird auch RS-232C-Port genannt.) Die meisten derartigen Geräte verfügen über zwei COM-Ports, über die häufig ein Modem, Terminaladapter oder Scanner angeschlossen wird. Sie verwenden in der Regel D-Sub 25-Pin oder D-Sub 9-Pin-Stecker.

CPCB

Abkürzung für Clock and PCI-Box Controller Board mit Systemuhr und Controllerschnittstelle.

Crossbar

Konzept, das den Datenstroms zwischen den Systemboards und IO Units steuert. Gleichbedeutend mit Speicher- und E-/A-Verbindung.

DDR2

Abkürzung für Double Data Rate 2. Standards für die neue Speichergeneration, die mit höheren Geschwindigkeiten und geringerem Stromverbrauch arbeiten als herkömmliche DDR-Speicher.

DIMM

Abkürzung für Dual Inline Memory Module. DIMMs kommen hauptsächlich in Notebooks zum Einsatz.

DP

Abkürzung für Dynamic Partitioning. Funktion zur dynamischen Hinzufügung, Löschung oder Ersetzung von Ressourcen wie CPUs, Hauptspeicher, PCI-Karten und IO Units im laufenden Systembetrieb einer Partition.

DVD-ROM

Abkürzung für Digital Versatile Disc - Read-Only Memory. Digitales Format zur Speicherung großer Datenmengen auf optischen Datenträgern.

ECC

Abkürzung für Error Checking and Correction. Prüft und korrigiert Fehler auf Basis der jeweiligen Fehlerkorrektur-Codes. Normalerweise sind mehr Diagnose- als Korrekturmaßnahmen verfügbar.

EFI

Abkürzung für Extendable Firmware Interface. Schnittstelle zwischen dem Betriebssystem und der Firmware. Das EFI wird zur Steuerung der Hardware verwendet.

EMEA

Abkürzung für „Europe, Middle East and Africa“ (Europa, Mittlerer Osten und Afrika)

Fibre Channel

Standard für serielle Schnittstellen. Der Fibre Channel benutzt Lichtwellenleiter für die Datenübertragung.

Firmware

In die Hardware integrierte Steuerungssoftware.

FWH

Abkürzung für Firmware Hub der Intel Corporation. Der FWH ist ein Flash Memory, in dem das SAL (BIOS) gespeichert wird. In den Systemen der PRIMEQUEST-Familie kommen zwei Arten von FWH zum Einsatz, einmal auf dem Systemboard und einmal in der IO Unit.

GAC

Abkürzung für Global Address Controller. Eine der von Fujitsu speziell für die PRIMEQUEST-Systemfamilie entwickelten ASICs.

GbE

Abkürzung für Gigabit Ethernet. Ethernet-Standard für extrem schnelle Datenübertragung bei Geschwindigkeiten bis 1 Gbps.

GDS

Kurzform für PRIMECLUSTER Global Disk Services.

GDX

Abkürzung für Global Data Xbar. Einer der von Fujitsu speziell für die PRIMEQUEST-Systemfamilie entwickelten ASICs.

GLS

Kurzform für PRIMECLUSTER Global Link Services.

GSWB

Abkürzung für Gigabit Switch Board. Das GSWB empfängt Daten im GbE-Format über eine Backplane von einer IO Unit und leitet diese an ein Ziel außerhalb des Schranks weiter.

HBA

Abkürzung für Host Bus Adapter

HDD

Abkürzung für Hard Disk Drive (Festplattenlaufwerk).

Hotplug

Verfahren zum Austausch von Komponenten bei laufendem Systembetrieb.

HTTP

Abkürzung für Hypertext Transfer Protocol. HTTP wird von Web-Servern und -Clients für die Datenübertragung verwendet.

I2C (Inter Integrated Circuit)

Protokoll für eine schnelle Datenübertragung zwischen integrierten Schaltkreisen.

Intel-Architektur

Generischer Begriff für die grundlegende Architektur der Intel-Mikroprozessoren.

IFT

Abkürzung für Instruction Fetch. Verfahren zu Lesen von Anweisungen, die im Speicher hinterlegt sind.

IO Unit

E-/A-Steuerungseinheit bestehend aus PCI-Slot, HDD, SCSI-Controller, GbE-Controller und anderen Ein-/Ausgabeschnittstellen.

IP-Adresse

Identifikationsnummer für die Verbindung eines Rechners zu einem IP-Netzwerk, etwa dem Internet oder einem Intranet

IPMI

Abkürzung für Intelligent Platform Management Interface. Standardisierte Schnittstellenspezifikationen, die es der SNMP- und der Verwaltungssoftware ermöglichen, einen beliebigen Server bzw. ein beliebiges Betriebssystem zu überwachen.

KVM-Einheit

Einheit, an die Tastatur, Maus und Bildschirm angeschlossen werden oder VGA-Schnittstelle für externe Ausgabe aus einer Partition.

LAN

Abkürzung für Local Area Network. Lokales Netzwerk, in dem Daten innerhalb eines Standortes beispielsweise über LWL-Kabel zwischen Rechnern und Peripheriegeräten aus getauscht werden können.

LDAP

Abkürzung für Lightweight Directory Access Protocol. Protokoll, mit dem in einem TCP/IP-Netzwerk auf Daten gegriffen wird, beispielsweise im Internet oder in einem Intranet.

LDX

Abkürzung für Local Data Xbar. Eine der von Fujitsu speziell für die PRIMEQUEST-Systemfamilie entwickelten ASICs.

LED

Abkürzung für Light Emitting Diode.

MAC-Adresse

Abkürzung für Media Access Control Address. Eine Hardware-Adresse, die einer bestimmten NIC (Network Interface Card) bzw. jedem einzelnen Port der Netzschnittstellengeräte, Switches oder Router auf der Systemplatine zugewiesen ist.

Management-LAN

Über das Management-LAN werden die MMBs mit Partitionen sowie mit dem Netzwerk außerhalb des Schranks verbunden.

MIB

Abkürzung für Management Information Base. Informationen, die von einem mit SNMP verwalteten Netzwerkgerät ausgegeben werden, um den Status des Gerätes an ein externes Ziel weiterzuleiten.

Middleware

Software, die auf einem Betriebssystem abläuft und den Anwendungen erweiterte Funktionen zur Verfügung stellt. Sie ist zwischen dem Betriebssystem und den Anwendungen angesiedelt.

MMB

Abkürzung für Management Board. Systemsteuerungseinheit, die die Hardware eines Schranks steuert und überwacht, die Partition verwaltet und das System initialisiert.

NIC

Abkürzung für Network Interface Card. Die NIC unterstützt die Netzwerkfunktionen.

Netzteil

Wandelt zur Versorgung des Systems Wechselstrom in Gleichstrom um.

NTP

Abkürzung für Network Time Protocol. Im Internet verwendetes Standardprotokoll für eine präzise Zeitangabe, das Leitungsgeschwindigkeiten und Belastungsschwankungen in den Pfaden berücksichtigt.

PAL

Abkürzung für Physical Abstract Layer. Firmware, die Startfunktionen für die Plattform und das Betriebssystem liefert.

Partition

System, das mit den Funktionen einer Verarbeitungseinheit ausgestattet ist. Jede Partition verfügt über Software-Ressourcen wie Betriebssystem und Anwendungen sowie über Hardware-Ressourcen wie Systemboards und IO Units.

PCI-Box

Erweiterungsgerät für PCI-Slots.

PCI-Hotplug

Verfahren, das einen Austausch von PCI-Karten bei laufendem Betrieb zulässt.

PCI

Abkürzung für Peripheral Component Interconnect. Bus-Architektur, die vom PCI SIG für die Verbindung von PC-Komponenten bereitgestellt wird.

PCIU

PCI-X-Karten Erweiterungsgerät, das in einer PCI-Box gemountet wird.

PEXU

PCI Express-Karten- Erweiterungsgerät, das in einer PCI-Box gemountet wird.

Plattform

Betriebssystem bzw. Umgebung, die als Basis für den Betrieb der Anwendungen dient.

POST

Abkürzung für Power-On Self Test. Hardware-Test, der automatisch abläuft, wenn ein Rechner eingeschaltet wird.

Private LAN

LAN, das für die interne Steuerung benutzt wird. Über das private LAN kommunizieren die auf der Hardware installierten Firmware-Programme miteinander. Die MMB-, GSWB- und BMC-Firmware auf den IO Units benutzen das private LAN für die Kommunikation. Das private LAN steht dem Betriebssystem und den Anwendungen nicht zur Verfügung.

PSA

Abkürzung für PRIMEQUEST Server Agent. Software, die die Konfiguration der PRIMEQUEST Partitionen überwacht und Hardwarefehler meldet.

PXE

PXE (Preboot eXecution Environment) Netzwerk-Boot-Standard basierend auf BIOS-Technologie zur Fernbedienung von Verwaltungsaufgaben wie Systemstart und BS-Installation/Update

RAID

Abkürzung für Redundant Array of Inexpensive Disks. Technologie, die die Zuverlässigkeit und Verarbeitungsgeschwindigkeit steigert, indem mehrere Festplatteneinheiten parallel eingesetzt werden und wie eine Festplatte behandelt werden.

REMCS*

Abkürzung für Remote Customer Support System. Fujitsus Remote Customer Support Service

Reserviertes Systemboard

Reserviertes Systemboard, das bei Ausfall eines anderen Systemboards zum Einsatz kommt.

Red Hat Enterprise Linux

Linux Betriebssystemversion der Red Hat, Inc.

SAF-TE

Abkürzung für SCSI Accessed Fault-Tolerant Enclosure.

SAL

Abkürzung für System Abstract Layer. Firmware, die Start- und Wiederherstellungsfunktionen unterstützt.

SAN

Abkürzung für Storage Area Network. Dediziertes Netzwerk, das einen Server mit Speichergeräten verbindet.

*: wird von Fujitsu Technology Solutions nicht unterstützt

SAS

Abkürzung für Serial Attached SCSI. Eine der Schnittstellen des SCSI-Standards zur Anbindung von Geräten wie Festplattenlaufwerken an den Computer. Die Daten werden per serieller Kommunikation übertragen.

SCSI

Abkürzung für Small Computer System Interface. Paralleler E-/A-Bus für Verbindungen zwischen PCs und ihren Peripheriegeräten. SCSI wurde 1986 von der American Standards Association eingeführt.

SDRAM

Abkürzung für Synchronous DRAM. Speicherstandard, der höhere Zugriffs-geschwindigkeiten bietet als DRAM.

SEL

Abkürzung für System Event Log. Logdatei, die Informationen enthält, die im laufenden Betrieb hier gespeichert werden.

SERDES

Abkürzung für Serializer Deserializer. Konvertiert niedrige Geschwindigkeiten in hohe Geschwindigkeiten.

Server System Manager

Management-Software zur integrierten Verwaltung mehrerer Server.

SIRMS

Abkürzung für Software Product Information Collection for Remote Maintenance Support. Sammelt Konfigurationsdaten über die in den PRIMEQUEST-Partitionen installierte Software.

S.M.A.R.T.

Abkürzung für Self-Monitoring Analysis Reporting Technology. Erlaubt einer Festplatte, sich selbst zu überwachen und das BIOS von erkannten Fehlern zu informieren.

SMP

Abkürzung für Symmetric Multiple Processor. System zur parallelen Verarbeitung, in dem alle Prozessoren auf gemeinsame Speicher-Ressourcen zugreifen.

SNMP

Abkürzung für Simple Network Management Protocol. TCP/IP-konformes Protokoll für die Verwaltung der Geräte in einem Netzwerk.

System Mirror Mode

Verfahren, nach dem Speicher, Systemverbindungen und interne Hardware-Komponenten eines Chipsatzes dupliziert werden, damit der Systembetrieb aufrecht erhalten werden kann, wenn eine der duplizierten Komponenten ausfällt.

Systemboard

Board, auf dem eine CPU und Speicher installiert sind.

SSL (Secure Sockets Layer)

Abkürzung für Secure Sockets Layer. Protokoll, nach dem Daten für die Übertragung verschlüsselt werden. SSL wurde von Netscape Communications Corp. entwickelt.

Systemwalker

Von Fujitsu entwickelte Middleware. Systemwalker ist eine integrierte Betriebsverwaltungssoftware.

Telnet

Standardverfahren für die entfernte Steuerung von Rechnern, die über ein TCP/IP-Netzwerk, etwa das Internet oder ein Intranet, angeschlossen sind.

USV

Abkürzung für Unterbrechungsfreie Stromversorgung. Sie schützt ein aktives System vor plötzlichen Stromunterbrechungen und den dadurch hervorgerufenen Datenverlusten.

USB

Abkürzung für Universal Serial Bus. Standard für den Anschluss von Geräten wie Tastatur und Maus.

VLAN (Virtuelles LAN)

Verfahren, nach dem die Ports eines Hubs logisch so gruppiert werden, dass jede Gruppe als unabhängiges LAN fungiert.

Web-UI (Web User Interface)

Graphische Benutzeroberfläche, die einen Webbrowser für die Darstellung von Informationen sowie für die Ausführung von Operationen durch den Benutzer verwendet.

XAI

Abkürzung für Xbar Address Interconnect Board. Überträgt Adressinformationen und steuert deren Übertragung zwischen den Systemboards und den Boards der IO Units.

XDI

Abkürzung für Xbar Data Interconnect Board. Steuert die Datenübertragung zwischen den Systemboards und den Boards der IO Units.

Stichwortverzeichnis

A

abmelden 2-9
Access Control
  Fenster 5-2
Access Control-Fenster 5-2
Add a Port
  Dialogfenster 4-77, 4-78, 4-92
Add SB/IOU to Partition-Fenster 2-58
Add User-Fenster 2-31
Advanced
  Registerblatt 4-75
aktives MMB 2-12
Alarm EMail Filtering Condition-Fenster . . . 2-28
Angaben zum System 2-11
anmelden 2-9
Anzeige des Wartungsstatus 2-12
Arbeitsablauf für den Start des Betriebs 1-1
ausschalten C-11, C-20

B

Backup EFI Configuration-Fenster 4-154
Backup MMB Configuration-Fenster 2-79
bedienerlose Installation 3-44, 3-55
Benutzerkonto 2-30, 2-32
  einrichten 2-32
  registrieren 2-30
Bestätigungsfenster 4-84
Bestätigungsmeldung 4-132
betrieb, Arbeitsablauf für den Start 1-1
Bisherige Versionen 5
Boot Control-Fenster 3-9, 3-16
Bundled-Software Package Installer A-4

C

Computer Management
  Fenster 4-70
config-Datei, Installation mit 3-14

D

Date/Time-Fenster 2-35, 4-136
Datum und Zeit
  einstellen 2-35
Deinstallation abgeschlossen 4-84, 4-98
deinstallieren
  PSA 4-21, 4-36, 4-64, 4-84, 4-98
  SIRMS 4-22, 4-37
Detected previous version of PSA 4-96
Dialogfenster
  Add a Port 4-92
diskdump 4-114
DNS-Server
  einrichten 2-24
DSNAP 4-125, 4-133, A-5
Dump Device 4-110
dump saving area, setting label 4-121
dump, manually collecting 4-123
Dump-Speicherbereich 4-112
Dump-Umgebung 4-1
  einrichten 4-110
  Linux 4-107
  Windows Server 2003 4-125
Duplizierung des Management-LAN 4-46

E

Edit Filter
  Fenster 5-4
Edit Filter-Fenster 5-3
EFI-Konfigurationsdaten 4-151, 4-154
ein- und ausschalten C-13
Ein-/Ausschalten C-1
Eingabe der Produktkennung 3-59
einschalten C-8, C-15
Export List-Fenster 4-152
Export-Fenster 4-154
Extended Mirror Mode 2-43

F

Fenster
  Select Features 4-97
Filter
  auswählen 5-2
  hinzufügen und bearbeiten 5-3
  löschen 5-4
Firewall 4-13, 4-28, 4-56, 4-77, 4-91
fjsnap A-3, A-6
Fujitsu Logo-Anzeige 2-11
Fujitsu Technology Solutions iii
. . . . . (siehe auch „Bisherige Versionen“)

G

Gigabit Switch Board (GSWB) 2-9

H

Hierarchieebene 2-13

High Reliability Tool 3-60
High-Reliability Tools Installer
Startfenster 3-61
Home 2-47
Home-Systemboard bzw. IO Unit festlegen 2-61
Home-Systemboard und IO Unit
einstellen 2-47
HTTP
einstellen 5-14
HTTPS 5-1
Einstellungen 5-15

I

Information-Fenster 2-77
Inhalt 2-15
Inhalt des Handbuchs i
Installation 3-1, B-1
erforderliche Gegenstände 1-3
mit unabhängigem KVM-Switch 3-13
PSA (Linux) 4-38
PSA (Windows Server 2003) 4-38
vor Beginn der 2-1
Voraussetzungen 3-4
installation
arbeitsablauf 1-1
required work 3-64
Installation abgeschlossen 4-83
installation floppy disk, creating 3-36
Installation mit config-Datei 3-7
Installation Support Tool A-4
Installation Support Tool for Windows A-11
Installationskonsole A-9
Installationsserver 3-21, 3-23, 3-31, 3-33
Installationsverfahren 3-1
Linux 3-2
Windows 3-3
Installationsvorbereitung 4-80, 4-81, 4-95
installieren
PSA (Linux) 4-3
PSA (Windows Server 2003) 4-65, 4-85
IO Unit 2-47, 2-55
IOU
hinzufügen 2-55
IOU and IOX
merging 2-53
splitting 2-53
IOU Split window PRIMEQUEST 520 2-53
IOU Split window PRIMEQUEST 580/540 . . 2-53
IOX
hinzufügen 2-55
IP-Adresse 2-3, F-1
festlegen 2-4
IP-Adresse des MMB 2-19

K

kdump collection, checking 4-123
kdump initial setting 4-119
kdump service, setting 4-122
Kernel-Dump 4-126
kexec-tool, installing 4-120
Konfiguration sichern 2-79
Konfigurationsdaten 2-19, 4-151
Konfigurationsinformationen 2-29
KVM
Installation über 3-6, 3-38, 3-49

L

Linux
Installation 3-6
Installationsverfahren 3-2
Linux sichern 4-142
Local Area Connection Properties
Dialogfenster 4-74

M

Management LAN Port Configuration-Fenster 2-41
Management-LAN . . . 2-30, 2-37, 4-4, 4-24, 4-39, ... 4-68, 4-88
Memory Dump-Datei 4-125
Menüleiste 2-12
Mirror Mode 2-47, 2-70
MMB
anmelden beim 2-9
IP-Adresse 2-21
mögliche Werte E-1
MMB anschließen und einrichten 2-3
MMB WUI 2-9, 2-10
MMB-Benutzerport, Position des 2-4
MMB-Konfigurationsdaten 2-79
MMB-Konsole 2-4
MMB-Netzwerk 2-19
einrichten 2-19, 2-21
Mode window 2-71

N

Network Interface-Fenster 2-20, 2-22
Network Protocol-Fenster . . 2-23, 5-5, 5-13, 5-15
Network Protocols
Fenster 5-6
Netzwerkadapter 4-72
Netzwerkeinstellungen 2-19
Neustart des Betriebssystems 3-48, 3-60
NTP-Betrieb bei PRIMEQUEST 4-134
NTP-Client 2-35, 4-1
NTP-Client einrichten 3-5, 4-134

NTP-Einstellung für eine Partition, die zu einer Domain gehört 4-141
NTP-Server einrichten 4-136

P

Paging-Datei 4-125
  einrichten 4-129
Partition 2-9
  Informationen anzeigen 2-77
  Informationen über 2-47
  initialisieren 2-47
  Reihenfolge der Einstellungen 2-47
  Reihenfolge der Konfiguration 2-47
Partition Configuration-Fenster . 2-56, 2-59, 2-69
Partition Home-Fenster 2-63
Partitionsname
  festlegen 2-47
Partitionsnamen
  festlegen 2-69
PC mit MMB-Konsole 2-4
PCI-Adressierungsmode 2-70
Performance Options
  Dialogfeld 4-130
Power Control
  Eingabefenster C-16
Power Control-Fenster . . 3-11, 3-17, 3-40, 3-51, ... C-15, C-20
PRIMECLUSTER GDS 4-143, 4-150
PRIMEQUEST Software Installer 3-61
PSA
  deinstallieren 4-21, 4-36, 4-64
  Installation (Linux) 4-38
  Installation (Windows Server 2003) 4-38
  installieren (Linux) 4-3
  installieren (Windows Server 2003) 4-65, 4-85
  Konfigurationsdaten 4-99, 4-151
  Menü 4-99
  Überwachung 4-99
  Update installieren 4-20, 4-35, 4-79, 4-94
  Vorgängerversion 4-82

R

rebooting system 4-122
Rechnername 2-30
Referenzhandbücher iii
Remote Server Management-Fenster 3-22, 3-32
Remove SB/IOU from Partition-Fenster . . . 2-60
reserviertes Systemboard
  einstellen 2-47, 2-63

S

S.M.A.R.T. 4-99
S.M.A.R.T., einrichten 4-99
S.M.A.R.T.-Fenster 4-101
SAN 3-26
SAN Boot Environment D-1
SAN Boot Environment einrichten D-2
SB
  hinzufügen 2-55
  teilen 2-51
  wieder verbinden 2-51
SB Split window 2-52
SB, IOU, und IOX
  teilen 2-51
  wieder verbinden 2-51
Schaltflächen 2-16
Schnappschuss 4-151
Select Features 4-83
  Fenster 4-97
SELinux 4-12, 4-27
Setup-Fenster 3-58
Sicherheitshinweis ix
Sicherheitsstufen 4-16
Sicherung des Betriebssystems 4-142
SIRMS
  deinstallieren 4-22, 4-37
  Update installieren 4-21, 4-36
SNMP
  einrichten 5-1, 5-5
SNMP Community
  Fenster 5-7
SNMP Community-Fenster 5-6
SNMP Trap
  Daten 5-9
SNMP Trap-Fenster 5-9
SNMP V3
  Einstellungen 5-11
SNMP v3 Configuration
  Daten 5-12
SNMP v3 Configuration-Fenster 5-11
SNMP-Trap 5-9
Software Support Guide A-11
SSH 5-1
  Einstellungen 5-14
  festlegen 5-13
Startup and Recovery
  Dialogfeld 4-128
Statusanzeige 2-15
Symbolik vi
System ausschalten C-7
System einschalten C-5
System Information-Fenster 2-33
System Power Control
  Eingabefenster C-10, C-14
System Power Control window C-10
System Power Control-Fenster . C-9, C-12, C-13
Systemboard 2-47, 2-55

Systemboard oder IO Unit
entfernen 2-47, 2-55
Systemboard und IO Unit
hinzufügen 2-47, 2-55
SystemcastWizard Lite 3-6, A-3, A-7
Installation mit 3-19, 3-29
installieren A-8
Konfiguration A-8
Systemeinstellungen A-5
Systemname 5-7
festlegen 2-33

T

Team Nummer 1
Eigenschaften 4-73
Teaming
Registerblatt 4-71
Team-Modus
Liste 4-72
Telnet
einstellen 2-23
Tera Term-Startfenster 3-46, 3-58
Trap-Ziel 4-14, 4-29, 4-57, 4-75, 4-89

U

Überschrift 2-15
Übertragung von E-Mails 2-28
Umgang mit diesem Produkt xv
Untermenü 2-13
unterstützte Betriebssysteme 3-1
Update abgeschlossen 4-81, 4-95
Update installieren
PSA 4-20, 4-35, 4-79, 4-94
SIRMS 4-21, 4-36
Update-Installation 4-80, 4-82, 4-96
USB/Video/DVD Switch-Fenster 3-8, 3-15, 3-39,
. 3-50
User List-Fenster 2-30

V

Verbindungseinstellungen 2-19
Virtual Memory
Dialogfeld 4-131
VLAN 2-30
VLAN in Management-LAN-Hub 2-37

W

Warnaufkleber xi
Warnhinweis ix
Warnhinweise
Konventionen vii
Watchdog 4-99
einrichten 4-101
Fenster 4-105
Watchdog-Fenster 4-104
WatchDog-Überwachung
Einschalten 4-78, 4-93
Watchdog-Überwachung
Einstellung 4-78
Web-UI-Fenster, Element 2-11
Windows Server 2003 . . . . . .4-65, 4-85
Windows sichern 4-142
Windows-Installation 3-3
Vorbereitungen 3-35
Windows-Partitionen sichern 4-150
Windows-Setup 3-37

X

XPAR, aktivieren 2-45

Y

YaST-Fenster 4-49

Z

Zugriffskontrolle einstellen 5-1, 5-2
Zustimmung zur Software-Lizenz 3-47, 3-59

Fujitsu Technology Solutions GmbH
Handbuchredaktion
33094 Paderborn

Fax: 0 700 / 372 00001

e-mail: manuals@ts.fujitsu.com
http://manuals.ts.fujitsu.com

Kritik
Anregungen
Korrekturen

Absender

Kommentar zu PRIMEQUEST 500A/500/400-Modellreihe
Installationshandbuch

U41632-J-Z816-5

Fujitsu Technology Solutions GmbH
Handbuchredaktion
33094 Paderborn

Fax: 0 700 / 372 00001

e-mail: manuals@ts.fujitsu.com
http://manuals.ts.fujitsu.com

Kritik
Anregungen
Korrekturen

Absender

Kommentar zu PRIMEQUEST 500A/500/400-Modellreihe
Installationshandbuch

U41632-J-Z816-5

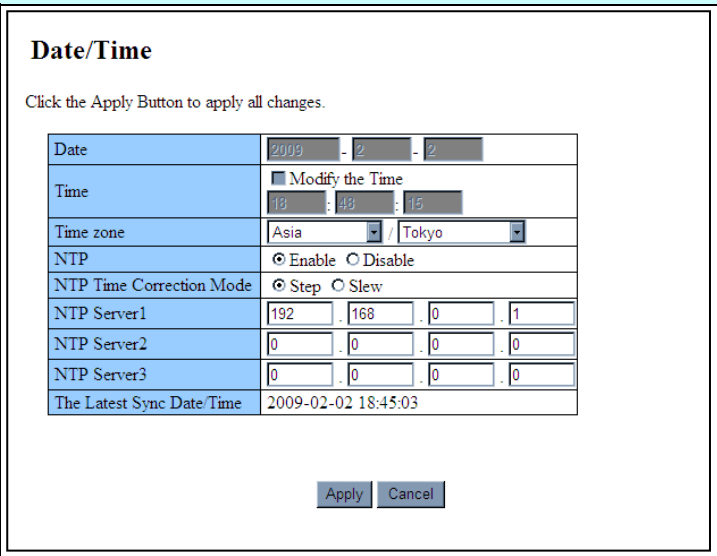
New items are marked yellow. All other items have been incorporated in the manual.

Table of corrections in PRIMEQUEST 500A/500/400 Series Installation Manual (C122-E001-10EN)

2009/6/18

Erroneous descriptions that were found in the manual have been corrected as shown below.

No.	Page	Item	Description	
1	2-23	2.2.3.5 SMTP settings	Incorrect	Note: A DNS server must be specified prior to specifying a fully qualified domain name (FQDN). You can specify it by selecting [Network Configuration] → [Network Interface].
			Correct	Note: - The From address for sending mail to the SMTP server when Alarm E-Mail is sent is as follows depending on the format set from [Network Configuration] → [Network Interface]: FQDN format root@[Hostname] Other than FQDN format root@[Hostname].[Hostname] The mail address that is set in From is used as the From address for sending mail to the receiving (To) address. - To specify an FQDN for the SMTP Server name, the DNS server must already be set. The DNS server can be set by selecting [Network Configuration] → [Network Interface].
2	2-33	2.2.4.4 Setting the date and time	Addition	(Addition of the following after step 3) • NTP operation specifications 1. Models covered by these specifications: PQ480/440/420 PQ580/540/520 PQ580A/540A/520A/520X/510A 2. Specifications of operations starting NTP client time synchronization The NTP client of the MMB starts time synchronization at the start of operation regardless of any time difference with the NTP server. The timing of the start of operation of the NTP client of the MMB is as follows: (1) It starts when the NTP service of the MMB is activated (when [Network Configuration] → [Date/Time] is selected from the MMB Web-UI, [Enable] is checked for [NTP] in [Date/Time], and the [Apply] button is clicked).

<table>
<tr><th>No.</th><th>Page</th><th>Item</th><th colspan="2">Description</th></tr>
<tr><td>2</td><td>2-33</td><td>2.2.4.4
Setting the date and time</td><td>Addition</td><td>


(2) With the NTP service of the MMB active, it starts when the MMB is reset, duplication of the MMB is switched, and the AC power is changed from OFF to ON.

3. Specifications of operations during NTP client time synchronization

The method for adjusting the NTP time varies depending on the firmware version and NTP operation mode (Step mode/Slew mode).

(1) In Step mode, if the time difference between the MMB and the NTP server being synchronized with is:

1) less than ±0.128 second, a slew adjustment is made (corrected maximally for 0.0005 second per second without reversal);

2) equal to or greater than ±0.128 second and less than ±1000 seconds, a step adjustment is made; (in this case, reversal is possible) or

3) equal to or greater than ±1000 seconds, the NTP function stops.

(2) In Slew mode, the operation varies depending on the version as follows. Note that the PQ480/440/420 have no Slew mode.

(a) PQ520: 3.24 and 3.25
PQ580/540: 3.24 and 3.25
PQ510A: 4.14 and earlier
PQ520A/520X: 4.17 and earlier
PQ580A/540A: 4.17 and earlier

If the time difference between the MMB and the NTP server being synchronized with is:

1) less than ±0.5 second, a slew adjustment is made (corrected maximally for 0.0005 second per second without reversal);
</td></tr>
</table>

No.	Page	Item	Description	
2	2-33	2.2.4.4 Setting the date and time	Addition	2) equal to or greater than ±0.5 second and less than ±600 seconds, the time is not adjusted; 3) equal to or greater than ±600 seconds and less than ±1000 seconds, a step adjustment is made; (in this case, reversal is possible) or 4) equal to or greater than ±1000 seconds, the NTP function stops. (b) PQ520: 3.26 and later PQ580/540: 3.26 and later PQ510A: 4.18 and later PQ520A/520X: 4.18 and later PQ580A/540A: 4.18 and later If the time difference between the MMB and the NTP server being synchronized with is: 1) less than ±600 seconds, a slew adjustment is made (corrected maximally for 0.0005 second per second without reversal); 2) equal to or greater than ±600 seconds and less than ±1000 seconds, a step adjustment is made; (in this case, reversal is possible) or 3) equal to or greater than ±1000 seconds, the NTP function stops. 4. Time polling interval The time is synchronized at an interval of 64 to 1024 seconds. The initial synchronization interval is 64 seconds. As the synchronization precision stabilizes, the interval increases in stages: 64 seconds → 128 seconds → 256 seconds → 512 seconds → 1024 seconds. (The algorithm for the increase in the synchronization interval complies with RFC 1305. For details, see Sections 3.4.2 through 3.4.9 of RFC 1305.) 5. NTP server stratum of the MMB The NTP server stratum of the MMB is stratum+1 of the external NTP server with which is it synchronized. If it is not synchronized with an external NTP server, this stratum is 5. 6. Accommodating leap seconds NTP of the MMB does not have a function for inserting leap seconds. Therefore, to have the MMB time support leap seconds, synchronize the MMB with an external NTP server that supports leap seconds. If the NTP client of the MMB is in Step mode and the time difference is equal to or greater than 0.128 second, the MMB time may undergo a step adjustment. This is possible even if the external NTP server gradually shifts the time to adjust for leap seconds. To prevent step adjustments during adjustments for leap seconds, use Slew mode.

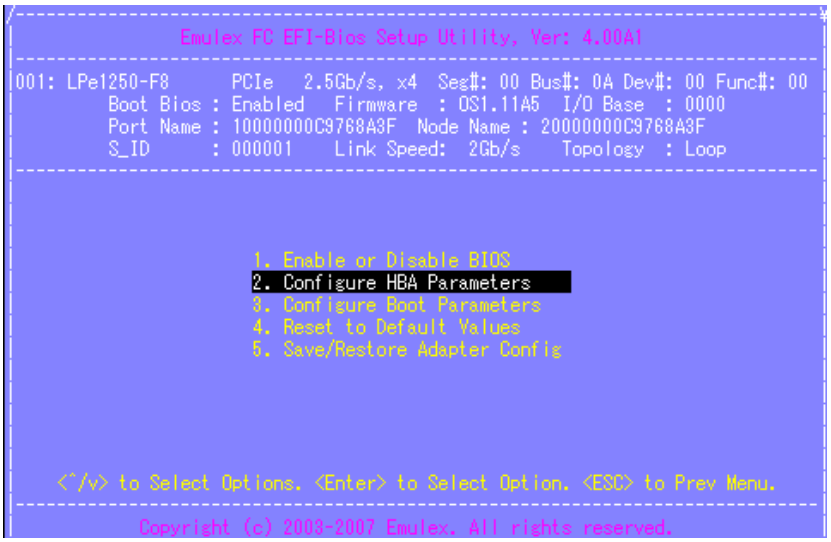
No.	Page	Item	Description	
2	2-33	2.2.4.4 Setting the date and time	Addition	However, if the time difference is equal to or greater than 0.5 second because of leap seconds, the time may fail to be adjusted. This is possible even during operation in Slew mode with the following firmware versions. For the relevant version, update the firmware to the latest version. - Firmware versions for which the time fails to be adjusted in Slew mode because of leap seconds PQ520: 3.24 and 3.25 PQ580/540: 3.24 and 3.25 PQ510A: 4.14 and earlier PQ520A/520X: 4.17 and earlier PQ580A/540A: 4.17 and earlier • Method of confirming the time synchronization with the NTP server For information on how to confirm that the time has been synchronized with the NTP server, consult your Fujitsu certified engineer or the support center.
3	2-63	2.5.6 Setting a reserved SB	Incorrect	3 [Replacement Condition] sets the condition that determines the timing at which the reserved SB is to be switched. (PRIMEQUEST 580A/540A/520A or PRIMEQUEST 500 series running MMB firmware whose version level is 3.24 or later)
			Correct	3 [Replacement Condition] sets the condition that determines the timing at which the reserved SB is to be switched. Note: For PRIMEQUEST 580A/540A/520A or PRIMEQUEST 500 series running MMB firmware whose version level is 3.24 or later, this item can be set. - SB failure: If an SB in the partition is degraded, it is replaced with the specified Reserved SB. - CPU/DIMM failure: If a CPU or DIMM on an SB in the partition is degraded, the SB is replaced with the specified Reserved SB. The default value is [CPU/DIMM failure].
4	4-3, 4-4	4.2 PSA Installation (Linux: Red Hat) (PRIMEQUEST 580A/540A/580/540/480/440)	Incorrect	- During PSA installation, the following modifications required for PSA operation are automatically put into effect: - Adding of settings to syslog.conf - Adding of settings to snmpd.conf - snmptrapd.conf file setup - Disabling of salinfo or salinfo_decode automatic startup setting (*1) - Disabling of smartd automatic startup setting - Adding of description to the services file (*2) *1 These automatic startup settings are disabled because of conflicts with some PSA functions. *2 Added Port: Port numbers are not checked for duplication when contents are added to the fj-webgate (24450) services file. Change them as necessary.

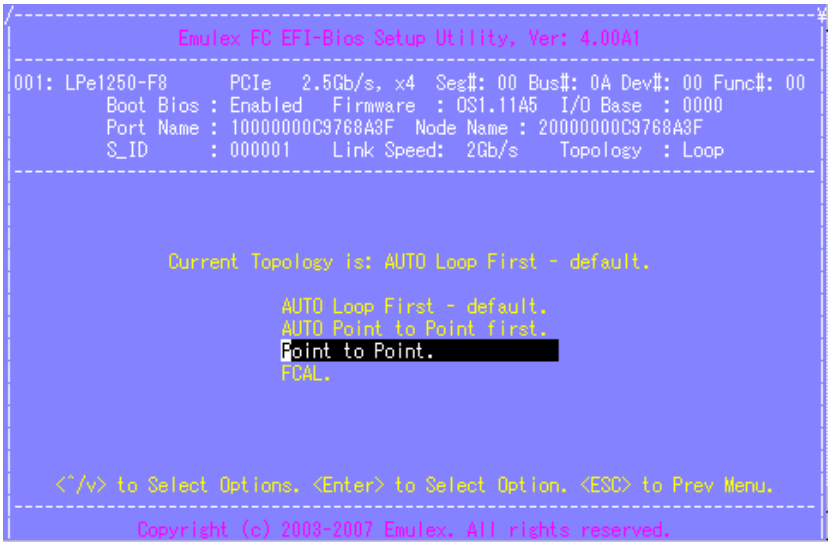
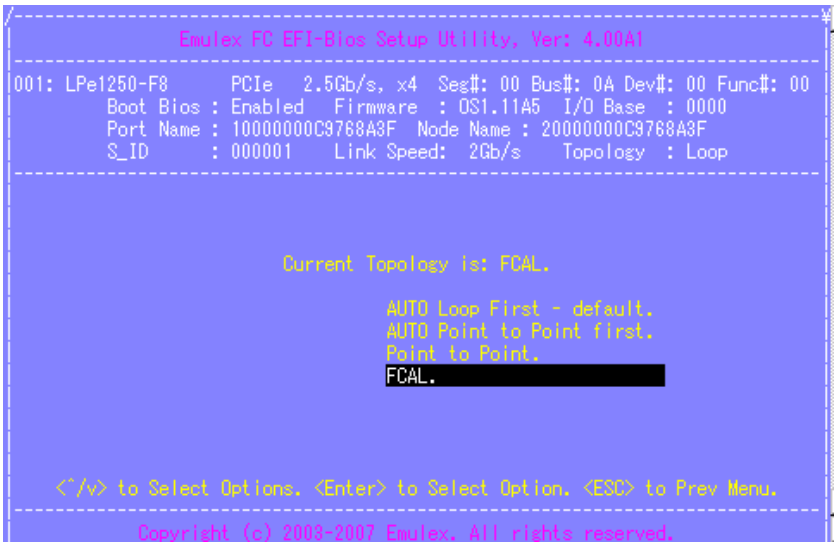
No.	Page	Item	Description	
4	4-3, 4-4	4.2 PSA Installation (Linux: Red Hat) (PRIMEQUEST 580A/540A/580/540/480/440)	Correct	- During PSA installation, the following modifications required for PSA operation are automatically put into effect: - Addition of the settings to syslog.conf file - Addition of the settings to snmpd.conf file - Addition of the settings to snmptrapd.conf file - Disabling of salinfo or salinfo_decode automatic startup setting (*1) - Disabling of smartd automatic startup setting (*1) - Addition of the settings to the services file (*2) - Correction of device types in the scsi.agent file (PSA1.16.2-xRHEL4 or later) (*3) - Addition of the settings to crontab file (PSA1.3.x-xRHEL4 to PSA1.6.x-xRHEL4) - Changing of snmptrapd boot option *1 These automatic startup settings are disabled because of conflicts with some PSA functions. *2 Added Port: Port numbers are not checked for duplication when the settings are added to the fj-webgate (24450) services file. Change them as necessary. *3 Corrections are made only for RHEL-AS4 (IPF).
5	4-20	4.2.8 PSA update installation	Addition	- Items automatically set during PSA update During PSA update, the following modifications required for PSA operation are automatically put into effect: - Correction of device types in the scsi.agent file (from PSA1.16.1-xRHEL4 or earlier to PSA1.16.2-xRHEL4 or later) - Deletion of the settings from crontab file (when PSA between PSA1.3.x-xRHEL4 and PSA1.6.x-xRHEL4 is updated to PSA1.7.x-xRHEL4 or later) - Changing of snmptrapd boot option (PSA1.19.1-x or later)
6	4-21	4.2.10 PSA uninstallation	Addition	- Items automatically set during uninstallation During PSA uninstallation, the following modifications are automatically put into effect: - Deletion of the settings from syslog.conf file - Deletion of the settings from snmpd.conf file - Deletion of the settings from snmptrapd.conf file - Enabling of salinfo or salinfo_decode automatic startup setting - Enabling of the smartd automatic startup setting - Deletion of the settings from services file - Deletion of settings from crontab file (PSA1.3.x-xRHEL4 to PSA1.6.x-xRHEL4) - Changing of snmptrapd boot option

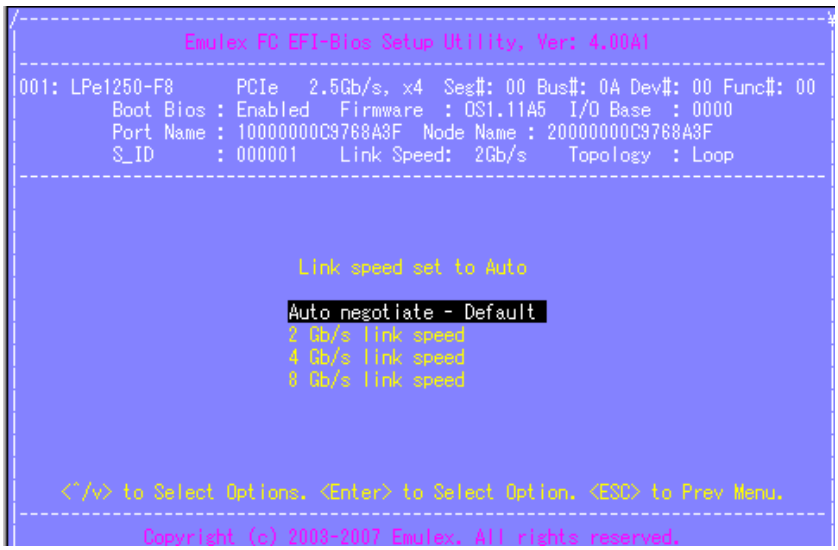
No.	Page	Item	Description	
7	4-22, 4-23	4.3 PSA Installation (Linux: Red Hat) (PRIMEQUEST 520A/520/420)	Incorrect	- During PSA installation, the following modifications required for PSA operation are automatically put into effect: - Adding of settings to syslog.conf - Adding of settings to snmpd.conf - snmptrapd.conf file setup - Disabling of salinfo or salinfo_decode automatic startup setting (*1) - Disabling of smartd automatic startup setting - Adding of description to the services file (*2) *1 These automatic startup settings are disabled because of conflicts with some PSA functions. *2 Added Port: Port numbers are not checked for duplication when contents are added to the fj-webgate (24450) services file. Change them as necessary.
			Correct	- During PSA installation, the following modifications required for PSA operation are automatically put into effect: - Addition of the settings to syslog.conf file - Addition of the settings to snmpd.conf file - Addition of the settings to snmptrapd.conf file - Disabling of salinfo or salinfo_decode automatic startup setting (*1) - Disabling of smartd automatic startup setting (*1) - Addition of the settings to the services file (*2) - Correction of device types in the scsi.agent file (PSA1.16.2-xRHEL4 or later) (*3) - Addition of the settings to crontab file (PSA1.3.x-xRHEL4 to PSA1.6.x-xRHEL4) - Changing of snmptrapd boot option *1 These automatic startup settings are disabled because of conflicts with some PSA functions. *2 Added Port: Port numbers are not checked for duplication when the settings are added to the fj-webgate (24450) services file. Change them as necessary. *3 Corrections are made only for RHEL-AS4 (IPF).
8	4-35	4.3.8 PSA update installation	Addition	- Items automatically set during PSA update During PSA update, the following modifications required for PSA operation are automatically put into effect: - Correction of device types in the scsi.agent file (from PSA1.16.1-xRHEL4 or earlier to PSA1.16.2-xRHEL4 or later) - Deletion of the settings from crontab file (when PSA between PSA1.3.x-xRHEL4 and PSA1.6.x-xRHEL4 is updated to PSA1.7.x-xRHEL4 or later) - Changing of snmptrapd boot option (PSA1.19.1-x or later)

No.	Page	Item	Description	
9	4-36	4.3.10 PSA uninstallation	Addition	- Items automatically set during uninstallation During PSA uninstallation, the following modifications are automatically put into effect: - Deletion of the settings from syslog.conf file - Deletion of the settings from snmpd.conf file - Deletion of the settings from snmptrapd.conf file - Enabling of the salinfo or salinfo_decode automatic startup setting - Enabling of the smartd automatic startup setting - Deletion of the settings from services file - Deletion of the settings from crontab file (PSA1.3.x-xRHEL4 to PSA1.6.x-xRHEL4) - Changing of snmptrapd boot option
10	4-37, 4-38	4.4 PSA Installation (Linux: SUSE) (PRIMEQUEST 500A/500/400 series common)	Incorrect	- During PSA installation, the following modifications required for PSA operation are automatically put into effect: - Adding of settings to syslog.conf - Adding of settings to snmpd.conf - snmptrapd.conf file setup - Disabling of salinfo_decode automatic startup setting (*1) - Disabling of smartd automatic startup setting - Adding of settings to the services file (*2) *1 These automatic startup settings are disabled because of conflicts with some PSA functions. *2 Added Port: Port numbers are not checked for duplication when contents are added to the fj-webgate (24450) services file. They may need to be changed.
			Correct	- During PSA installation, the following modifications required for PSA operation are automatically put into effect: - Addition of the settings to syslog.conf file - Addition of the settings to snmpd.conf file - Addition of the settings to snmptrapd.conf file - Disabling of salinfo_decode automatic startup setting (*1) - Disabling of smartd automatic startup setting (*1) - Addition of the settings to the services file (*2) - Changing of snmptrapd boot option *1 These automatic startup settings are disabled because of conflicts with some PSA functions. *2 Added Port: Port numbers are not checked for duplication when the settings are added to the fj-webgate (24450) services file. Change them as necessary.

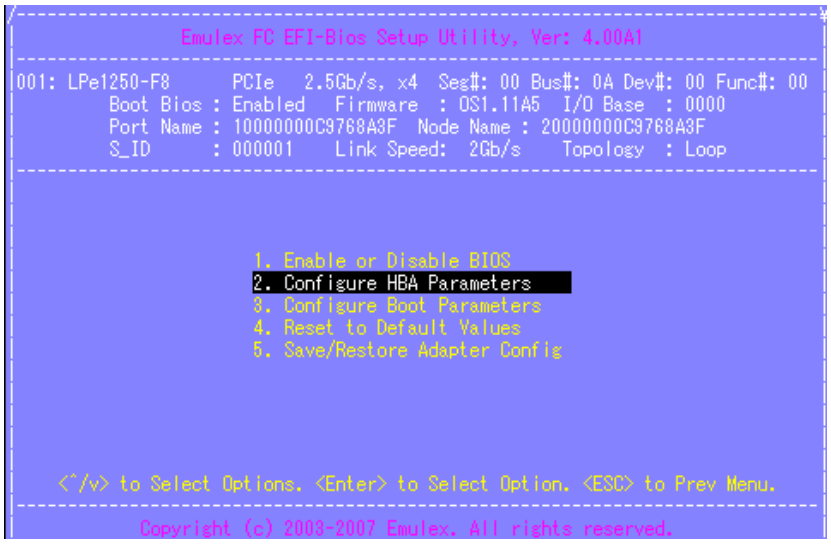
<table>
<tr><th>No.</th><th>Page</th><th>Item</th><th colspan="2">Description</th></tr>
<tr><td>11</td><td>4-65</td><td>4.4.9
PSA
uninstallation</td><td>Addition</td><td>- Items automatically set during uninstallation
During PSA uninstallation, the following modifications are automatically put into effect:
- Deletion of the settings from syslog.conf file
- Deletion of the settings from snmpd.conf file
- Deletion of the settings from snmptrapd.conf file
- Enabling of the salinfo_decode automatic startup setting
- Enabling of the smartd automatic startup setting
- Deletion of the settings from services file
- Changing of snmptrapd boot option</td></tr>
<tr><td rowspan="2">12</td><td rowspan="2">4-90</td><td rowspan="2">4.6.4
Windows
firewall setting</td><td>Incorrect</td><td>- TCP port used for SNMP: 161 port</td></tr>
<tr><td>Correct</td><td>- UDP port used for SNMP: 161 port</td></tr>
<tr><td rowspan="2">13</td><td rowspan="2">5-8</td><td rowspan="2">Table 5.4
Displayed and setting items in the [SNMP Community] window</td><td>Incorrect</td><td><table><tr><td>IP Address/MASK</td><td>Sets an access-enabled IP address or network address.</td></tr></table></td></tr>
<tr><td>Correct</td><td><table><tr><td>IP Address/MASK</td><td>Sets an access-enabled IP address or network address.
The IP address and subnet mask together specify a subnet as follows:
<subnet-IP-address>/<number-of-subnet-mask-bits>
For example, the subnet with the IP address 10.10.10.0 and the subnet mask 255.255.255.0 is specified as follows:
10.10.10.0/24</td></tr></table></td></tr>
<tr><td rowspan="2">14</td><td rowspan="2">D-7</td><td rowspan="2">D.4.4
Configuring the EFI driver</td><td>Incorrect</td><td>- Configuring the EFI driver (3.11a4 version/3.11x1 version) (→D.4.4.2)</td></tr>
<tr><td>Correct</td><td>- Configuring the EFI driver (3.11a4 version/3.11x1 version or later) (→D.4.4.2)</td></tr>
<tr><td>15</td><td>D-10</td><td>D.4.4.1
Configuring the EFI driver (3.10a6 version)</td><td>Incorrect</td><td>10 Press the [Esc] key once to return to the window displayed in step 6.
11 Specify the boot device.
Select [3. Configure Boot Parameters] from the menu displayed in step 6.
The following menu is displayed:</td></tr>
</table>

No.	Page	Item	Description	
			Correct	10 Press the [Esc] key once to return to the window displayed in step 6. 11 Set the topology. Make the following EFI-Bios settings according to the connection type (Fabric connection or FCAL connection). *The following screenshot of the EFI-Bios Utility screen corresponds to a configuration with two Single FC cards and two Dual FC cards. < Fabric > Select the card whose setting you want to change. 1) Select [Configure HBA Parameters].  2) Select [Topology Selection].

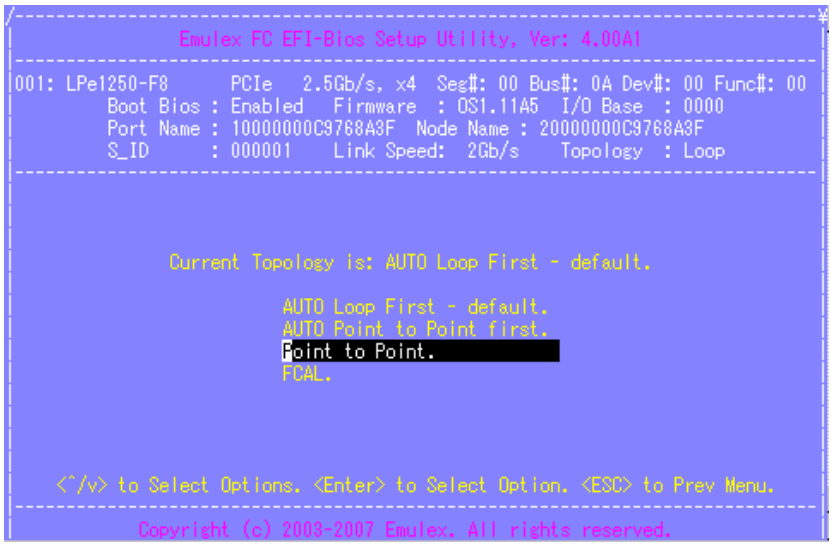
No.	Page	Item	Description
			3) Select [Point to Point].  <FCAL > Select the card whose settings you want to change, in the same way as the above 1) and 2) for a Fabric connection. 4) Select [FCAL].  12 Set the link speed. Make the following EFI-Bios settings according to the Link Speed for the connection (2, 4, or 8 Gbps). On the window that is displayed in 3) or 4) of step 11, first press the [Esc] key once to return to the previous window. In the window displayed in 2), select [4. Force Link Speed]. The default setting is [Auto negotiate - Default]. Select the Link Speed setting appropriate to your environment.

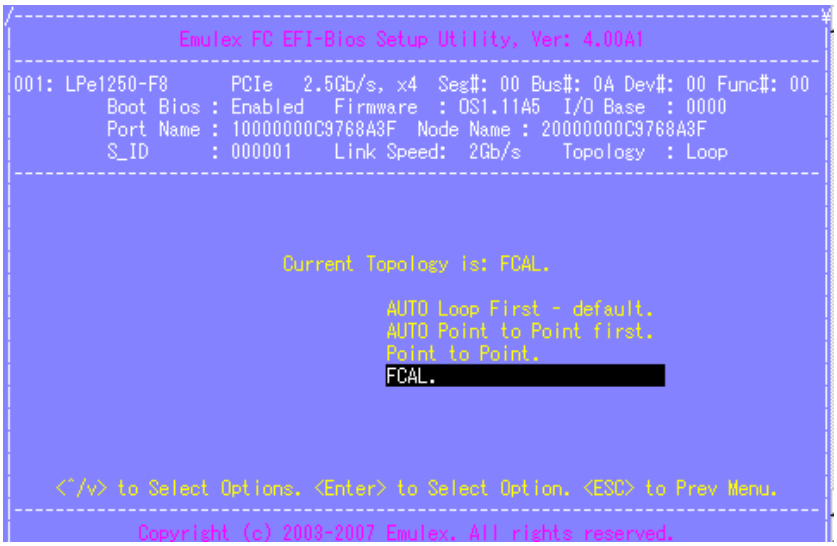
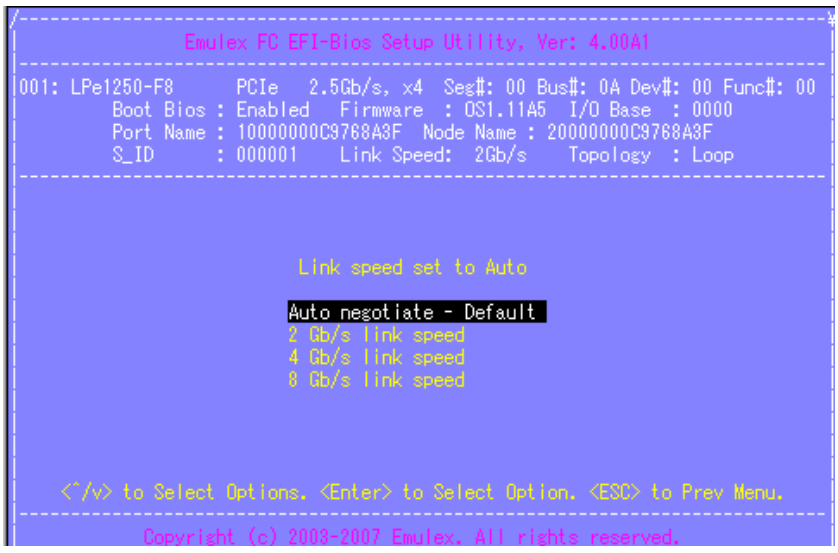
No.	Page	Item	Description
			*If the EFI driver version is 3.10a6, 3.11a4, or 3.11x1, Link Speed cannot be set. In this case, the appropriate setting is [Auto negotiate]. Use the system as is. (8GFC)  (4GFC)

No.	Page	Item	Description
			(2GFC) 13 Change the setting for the opposed devices in the connection (Fibre Channel switch/ ETERNUS disk array). It is necessary to change the settings on the devices at the opposite end of the connection to match the fixed settings on the Fibre Channel card. (This applies both to Fibre Channel switches and ETERNUS disk arrays.) For details, see ETERNUS Disk Storage System Settings / 2.1.1 Setting the To-server Connection Type (Setting the CA Parameters) of *ETERNUS Disk Storage System Server Connection Guide (Fibre Channel)*. 14 Set the boot device. Select [3. Configure Boot Parameters] in the menu that is available in step 6 of the procedure. The following menu will be displayed.

<table>
<tr><th>No.</th><th>Page</th><th>Item</th><th colspan="2">Description</th></tr>
<tr><td rowspan="2">16</td><td rowspan="2">D-12</td><td rowspan="2">D.4.4.2 Configuring the EFI driver (3.11a4 version/3.11x1 version)</td><td>Incorrect</td><td>D.4.4.2 Configuring the EFI driver (3.11a4 version/3.11x1 version)</td></tr>
<tr><td>Correct</td><td>D.4.4.2 Configuring the EFI driver (3.11a4 version/3.11x1 version or later)</td></tr>
<tr><td rowspan="2">17</td><td rowspan="2">D-15</td><td rowspan="2">D.4.4.2 Configuring the EFI driver (3.11a4 version/3.11x1 version)</td><td>Incorrect</td><td>10 Press the [Esc] key once to return to the window displayed in step 6.
11 Specify the boot device.
Select [3. Configure Boot Parameters] from the menu displayed in step 6.
The following menu is displayed:</td></tr>
<tr><td>Correct</td><td>10 Press the [Esc] key once to return to the window displayed in step 6.
11 Set the topology.
Make the following EFI-Bios settings according to the connection type (Fabric connection or FCAL connection).
*The following screenshot of the EFI-Bios Utility screen corresponds to a configuration with two Single FC cards and two Dual FC cards.
< Fabric >
Select the card whose setting you want to change.
1) Select [Configure HBA Parameters].
 

2) Select [Topology Selection].</td></tr>
</table>

No.	Page	Item	Description
			 3) Select [Point to Point].  <FCAL > Select the card whose settings you want to change, in the same way as the above 1) and 2) for a Fabric connection. 4) Select [FCAL].

No.	Page	Item	Description
			 12 Set the link speed. Make the following EFI-Bios settings according to the Link Speed for the connection (2, 4, or 8 Gbps). On the window that is displayed in 3) or 4) of step 11, first press the [Esc] key once to return to the previous window. In the window displayed in 2), select [4. Force Link Speed]. The default setting is [Auto negotiate – Default]. Select the Link Speed setting appropriate to your environment. *If the EFI driver version is 3.10a6, 3.11a4, or 3.11x1, Link Speed cannot be set. In this case, the appropriate setting is [Auto negotiate]. Use the system as is. (8GFC) 

No.	Page	Item	Description

(4GFC)

Emulex FC EFI-Bios Setup Utility, Ver: 4.00A1
002: LPe11002-M4 PCIe 2.5Gb/s, x4 Seg#: 00 Bus#: 0C Dev#: 00 Func#: 00
Boot Bios : Enabled Firmware : ZS2.80A4 I/O Base : 0000
Port Name : 10000000C96A8E00 Node Name : 20000000C96A8E00
S_ID : 000001 Link Speed: NA Topology : Invalid
Link speed set to Auto
Auto negotiate - Default
1 Gb/s link speed
2 Gb/s link speed
4 Gb/s link speed
<^/v> to Select Options. <Enter> to Select Option. <ESC> to Prev Menu.
Copyright (c) 2003-2007 Emulex. All rights reserved.

(2GFC)

Emulex FC EFI-Bios Setup Utility, Ver: 4.00A1
004: LP10000 PCI-X 133MHz Seg#: 00 Bus#: 23 Dev#: 01 Func#: 00
Boot Bios : Enabled Firmware : TS1.91A1 I/O Base : 0000
Port Name : 10000000C945CA82 Node Name : 20000000C945CA82
S_ID : 000001 Link Speed: NA Topology : Invalid
Link speed set to Auto
Auto negotiate - Default
1 Gb/s link speed
2 Gb/s link speed
<^/v> to Select Options. <Enter> to Select Option. <ESC> to Prev Menu.
Copyright (c) 2003-2007 Emulex. All rights reserved.

13 Change the setting for the opposed devices in the connection (Fibre Channel switch/ ETERNUS disk array).

It is necessary to change the settings on the devices at the opposite end of the connection to match the fixed settings on the Fibre Channel card. (This applies both to Fibre Channel switches and ETERNUS disk arrays.)

For details, see ETERNUS Disk Storage System Settings / 2.1.1 Setting the To-server Connection Type (Setting the CA Parameters) of *ETERNUS Disk Storage System Server Connection Guide (Fibre Channel)*.

14 Set the boot device.

Select [3. Configure Boot Parameters] in the menu that is available in step 6 of the procedure. The following menu will be displayed.

(End of table)